ANNUAL EDITION - RSAConference2017

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION



foreword by

Linda Gray Martin

Director & General Manager,
RSA Conference

2017 PREDICTIONS

CYBERSECURITY TRENDS

BREACH PREVENTION

NEXT GEN INFOSEC

CDM ANNUAL AWARDS

SECURE YOUR IT WORLD. THE PREMIER SOURCE FOR IT SECURITY INFORMATION

ANNUAL CDM EDITION

DISCOVERING INFOSEC INNOVATION

THAT'S OUR MISSION & PASSION

CYBER DEFENSE MAGAZINE

WELCOME ABOARD

We're honored to bring you our 5th Annual edition of Cyber Defense Magazine, exclusively in print at the RSA Conference 2017. While this may only be our sixth year at RSA, some of our team members have been coming to this amazing INFOSEC conference for longer than they wish to admit. The RSA Conference is constantly evolving to keep pace with an ever changing cyber security landscape. It look like 2017 will be another year of massive breaches, with a new focus on Small to Medium Size Enterprises (SME s) who are less secure and have less budgets. We re seeing a growing number of successful ransomware attacks as well as zero-day remote access Trojans (RATs). We ve even seen many cyber crime attacks become politicized, where, even without complete analysis, various organizations are blaming the Russian government on the results of the US Presidential Elections.

From Hactivism and Watchdog groups like Wikileaks gaining momentum to Cyber Espionage and Cyber Crime, you ll find some of the best and most innovative speakers, technologies, products and services here at the RSA Conference to help you get one step ahead of the next threat to your own organization. This year, RSA Conference 2017 expects more than 30,000 attendees who are looking for solutions just like you. What a great opportunity to mingle, network, share ideas and learn new ways of thinking about the cyber threat problem. If you are one of the lucky attendees who convinced your CEO that this is a must attend show - you did the right thing. You've come to the right place. This is where we learn, share new ideas, see new technologies and develop our plans to stay one step ahead of the next threat, together. You'll also find that's what Cyber Defense Magazine is all about, continuing to focus on best practices and solutions for you - our monthly Cyber Warnings e-magazines cover hot INFOSEC topics with some of the best advice from experts. Our Annual Edition, exclusively in print, only at RSA Conference, contains some of the most informative articles and awards for products and solutions that will help you find the solution you need.

Take a peek inside our annual edition and you'll see we're covering some of the most interesting 'hot' topics including Adaptive Security, Endpoint Protection, Security Automation, our Editor's Cybersecurity Predictions for 2017 and so much more. If you don t know Pierluigi Paganini, you should – our Editor is one of the Global Infosec Thought leaders. He s always on his game and his predictions usually come true, so read and re-read his view on what s coming our way in 2017. I also wanted to thank our Executive Producer and Co-owner of the Magazine – Gary S. Miliefsky (who happens to be my dad, and a fellow white hat). While he s busy growing his latest venture, SnoopWall, Inc., the breach prevention company, we re growing CDM with your help and continued support Without his original vision and leadership, CDM wouldn t be here. Without your amazing support, we wouldn t be here. For that, we are sincerely grateful.

To our faithful readers and RSA Conference 2017 attendees, we appreciate you.

Sincerely,
Stevin Miliefsky, President

CONTENTS

Overcoming the Challenges of the Cybersecurity Skills Gap……..…….4

The Future of Cyber Security: Risk-Based Attack Surface Validation and Remediation……...…….…..…..8

Reinventing Software Forensics with Static Analysis…..……...…..……12

Automating Data Collection to Improve Cyber Security……..…….15

The Current State of ICS Cyber Security……..…..18

The Mirage of Data Security Compliance and the Federal Trade Commission……..……23

Startups with Information Security in Mind at Startup..…..…..……27

Amazon's Echo May Be Sending Its Sound Waves Into The Court Room As Our First "Smart Witness"…….….30

Runtime Application Self-Protection (RASP) - The Future of Application Security…..…….…..…..…34

Sophistication Of Cyber-attacks Creates Era Of Internet Security As A Right……...…..…….…...…...……..……38

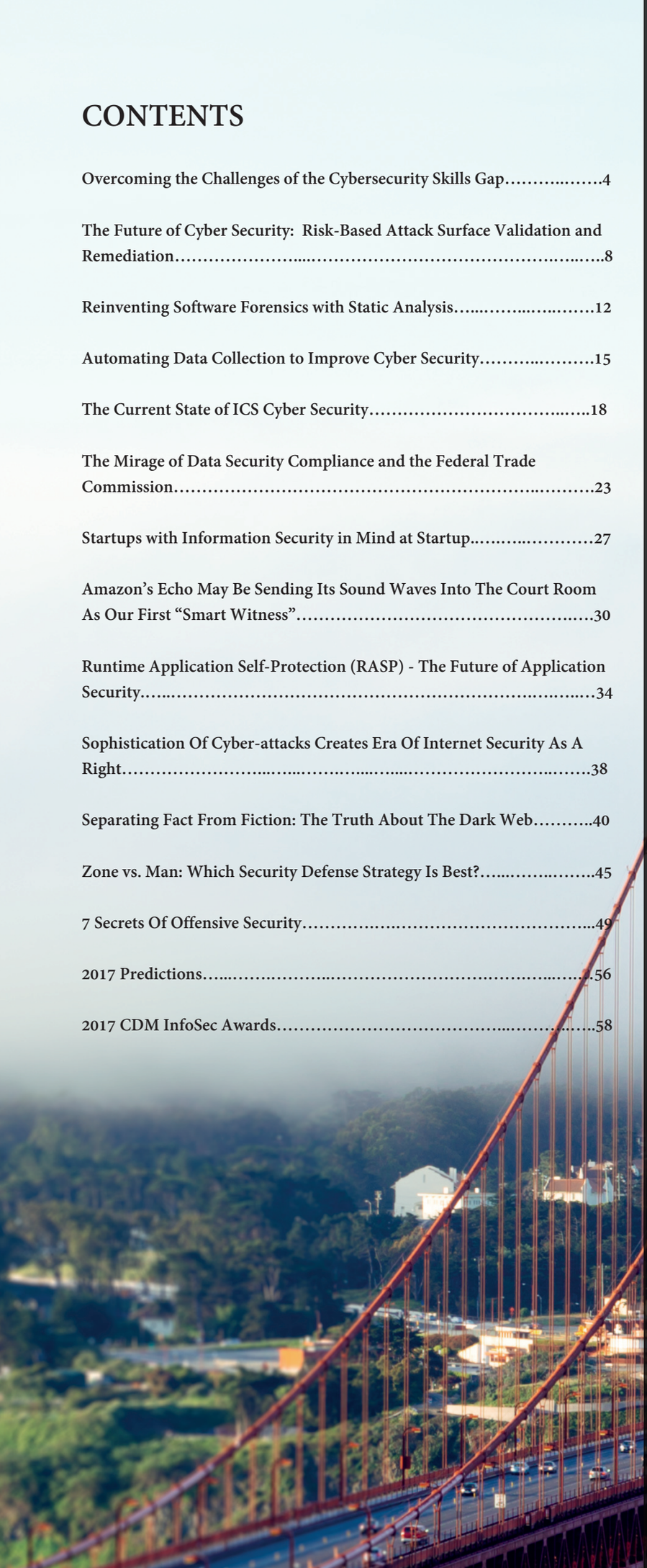
Separating Fact From Fiction: The Truth About The Dark Web……..40

Zone vs. Man: Which Security Defense Strategy Is Best?…...……..……..45

7 Secrets Of Offensive Security……..……..49

2017 Predictions…...…….……...……..…….56

2017 CDM InfoSec Awards……...……..58



Cyber Defense Magazine (CDM) is distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats. All electronic editions are available for FREE, always. No strings attached. Annual print editions of CDM are distributed exclusively at the RSA Conference each year.

PRESIDENT
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

EXECUTIVE PRODUCER
Gary S. Miliefsky, FMDHS, CISSP®
garym@cyberdefensemagazine.com

EDITOR-IN-CHIEF
Pierluigi Paganini, CEH
pierluigi.Paganini@cyberdefensemagazine.com

ADVERTISING
Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS
Linda Gray Martin
Tom Gilheany
Torsten George
Bill Graham
Jay Botelho
Barak Perelman
Michael Daugherty
Kip James
Andrew L. Rossow Esq.
John Matthew Holt
Luis Corrons
Emily Wilson
Dr. Clare Gollnick
Kim Ellery
Gary S. Miliefsky
Pierluigi Paganini

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: +1-800-518-5248
Fax: +1-702-703-5505
SKYPE: cyber.defense
Email: marketing@cyberdefensemagazine.com

Copyright (C) 2017, Cyber Defense Magazine (CDM), a publication of STEVEN G. SAMUELS LLC
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107 USA
EIN: 454-18-8465, DUNS# 078358935.



RSA® Conference2017

Linda Gray Martin,
Director & General Manager, RSA Conference

RSA® Conference, the world s leading information security conferences and expositions, is once again taking over San Francisco from February 13- 17, 2017 to drive the global narrative about security. This annual event is one of the largest of its kind with thousands of security professionals coming together with hundreds of media, analysts and exhibitors every year.

Each year during RSA Conference, leaders from around the world gather to share best practices, challenge each other, and discover new products to keep our organizations safe from cyber attacks. In 2017 we ll gather around the theme **Power of Opportunity**, highlighting the inclusive atmosphere of sharing and exploration necessary for our industry to unite and tackle issues beyond those we face in our everyday jobs.

When we remove the boundaries of what can and can t be done, we open ourselves to new opportunities. There s a Zen approach to learning put forth by Shunryu Suzuki that one should pursue even the most advanced study with the mindset of a beginner. In the beginner s mind, there are many possibilities. In the expert s mind, there are few. When we embrace more possibilities, inspiration follows. RSA Conference is a place where ideas are given the opportunity to cascade and grow—like the ripple effect of tossing a single stone into the water. After a stone is tossed at RSAC, the rippling what ifs spark new ways of thinking and generate new courses to pursue. From there, the power of opportunity takes on the challenges of the digital age.

Opportunity is a compelling and influential thing. It opens the door and invites all inside to reimagine and reinvent. It allows us to come together as a whole to collaborate on modern innovations. It encourages everyone to embrace new and unique perspectives from a diverse base of sources and people; often the best minds in the industry, from a multitude of backgrounds. And it allows for a dynamic exchange of ideas amongst peers. Every day, all of us are working to tackle the ongoing security challenges we face. Collaboration, information and an open dialogue are some of the best tools we can utilize to keep ourselves safe – both at work and personally.

We hope that you will take this year s conference as an opportunity to both challenge your own thinking and that of your peers. We look forward to seeing and hearing from you throughout the week

Linda Gray Martin,
Director & General Manager, RSA Conference

OVERCOMING THE CHALLENGES OF THE CYBERSECURITY SKILLS GAP



TOM GILHEANY, CISSP

Product Manager,
Cisco Systems

Digital transformation is sweeping across the business landscape, offering real opportunities for streamlined processes, improved customer experiences, innovation and growth into new markets. Businesses, in their desire to gain any competitive advantage possible, are embracing digitization as quickly as their IT teams can manage it.

> *"The growing interconnectedness of human beings, information, and machines makes it easier for criminals to steal valuable data, such as trade secrets, future product design plans, non-public financial data and private customer records"*

The combined trends of mobility, big data, cloud, collaboration technologies and the Internet of Things (IoT) are creating many challenges as well. One of main challenges has to do with cybercrime. The growing interconnectedness of human beings, information, and machines makes it easier for criminals to steal valuable data, such as trade secrets, future product design plans, non-public financial data and private customer records. This interconnectedness also makes it easier to nefarious actors to take control of critical machines or misappropriate resources and technology for malicious purposes.

One factor that makes fighting cybercrime even more difficult is the huge amount of data generated daily by network-connected devices, which produce 277 times more data daily than do people, with much of that data not verified by humans. That s a virtual goldmine of information. In addition, the controls of IoT things can be controlled remotely if hacked, adding a new layer of risk.

Organizations must work to keep these systems and data, which is often sensitive, proprietary or confidential in nature, away from professional cybercriminals who seek monetary gain from exploiting the digital expansion. While thieves reap big rewards for stealing data, businesses and other entities pay a rising price. The Ponemon Institute looked at 383 companies in 12 countries in 2016 and found that the average consolidated total cost of a data breach is $4 million This figure represents several factors. First, thieves are able to steal – or ransom – much more value in terms of information assets, than before. Second, newer regulatory penalties have been increased – or created – that place additional requirements on organizations to protect their data and digital systems.

It take experts with the advanced skills and knowledge to connect networks, devices, and people securely in order to keep data, networks, machines, and people safe. Businesses need properly trained and certified personnel to design and build secure infrastructure, as well as to detect and respond to increasingly insidious cybersecurity threats. Yesterday s knowledge (and security techniques) don t cut it anymore.

Another factor complicating the fight against cybercrime is the security skills talent gap. There simply are not enough trained and certified IT workers to fulfill soaring demand for digital security expertise. The Bureau of Labor Statistics predicts that demand for cybersecurity analysts will grow 18 percent by 2024 in the United States alone.

The Security Talent Crisis

Many new technologies will be quickly adopted along the inexorable march to digitization: software-defined networking (SDN), mobility, enhanced security, flexible access and virtualization, while taking full advantage of cloud deployment models. Each new technology affects the others, and all of them entail new security concerns. For

example, an organization cannot deploy and fully leverage newer technologies, such as cloud, without a clear understanding of the resulting changes to their security posture.

> *"The world is becoming increasingly controlled by automation software, which means the security environment of these systems also is no longer static—it's a moving target"*

Intelligence and automation become the main focus during digital transformation. The world is becoming increasingly controlled by automation software, which means the security environment of these systems also is no longer static—it s a moving target. The old IT security paradigm of set it and forget it suffices no longer now that threats are dynamic, evolving, and striking from anywhere and everywhere. In the new digital era, security is everyone s concern, job title notwithstanding. Every facet of IT must be viewed and evaluated through the lens of security.

Cybercriminals are constantly changing and improving their tactics, and their continuously evolving attempts to breach network security, steal data, and gain control of systems have frequently outstripped the ability of IT and security professionals to protect the growing amount of data across a growing number of systems and users.

The shortfall of IT workers who have skills relevant to today s threats is one of the biggest factors affecting an organization s security posture. A recently published study of the cybersecurity skills shortage was conducted by Intel Security with the Center for Strategic and International Studies (CSIS). It surveyed 775 IT decision-makers in public and private sector organizations across eight countries: Australia, France, Germany, Israel, Japan, Mexico, the UK and the U.S. It is shocking and worrisome that 82 percent of those polled reported a shortage of cybersecurity skills in their organizations. This acute talent shortage shows up in many ways:

- Lack of talent in critical roles
- Higher costs to retain talent
- Inability of staff to remain current with the evolving threat landscape

There are several contributors to this issue. For one thing, the security landscape is increasingly complex. By way of example, a typical enterprise has between 30 and 40 different security vendors in its network, creating a patchwork of solutions that each needs to be updated and managed independently, increasing the chances that an attacker can exploit the weak spots in this piecemeal defense.

Another contributing factor is how cyberattacks themselves are changing, now often generated by organized cyber-criminals or government-backed organizations with large budgets and teams. In addition, by connecting more and different types of devices, the IoT opens up new and unforeseen ways to access systems and information. Today more than 10 billion connected devices are running 77 billion applications. By 2020, there will be more than 50 billion connected devices and more than 500 billion a decade later. That s a huge growth potential not only for enterprises, but also for criminals. With IoT, criminals are now able to take control of devices for ransom or repurposing in addition to stealing data outright.

People Make the Security Difference

However, all is not lost; help is available. Organizations can protect themselves against the new security challenges brought about by digitization by understanding their needs and investing in their people.

IT professionals today need to know how to identify malicious behaviors, correlate different activities that

enhance the fidelity of the analysis and quickly classify events by separating out false positives from true positives. Some of the security skills in demand include:

- Secure software development
- Secure network design
- Attack mitigation expertise
- Threat detection
- Application security knowledge
- Forensic analysis to track the origins of breaches
- Penetration testing & security auditing
- Mobile security expertise
- Security operations center monitoring
- Cloud and data center protection expertise

Operations specialists need to be part of the security team, in addition to the more traditional perimeter security experts, identity managers and security architects. The concept of federated security teams is gaining more acceptance, as the attack methods used by cybercriminals are diversifying as well. A security operations workforce will monitor IT security systems, detect cyberattacks, gather and analyze evidence, correlate information, and coordinate responses to cyber incidents. They can determine whether an intrusion or security-related event has occurred or is currently occurring. In addition, they can analyze telemetry data commonly obtained through various feeds that the analysts use to correlate logs together into related chains of events, allowing them to sort out relevant conversations taking place around an event. By hiring and training employees with these specialized skills, organizations can enhance their existing security teams with another defense against the newly evolving cybersecurity challenges brought by digitization.

Worth the Investment

Network attacks come from within and without. It takes skilled engineers to design comprehensive detection mechanisms and analysts/investigators to comb through all information sources to find the needle in the haystack. Finding and training the next generation of security talent is the next step.

To overcome the cybersecurity talent gap, a recent CSIS global study offered several recommendations:

- Accept non-traditional sources of education
- Diversify the cybersecurity field
- Provide more opportunities for external training
- Identify technology that can provide intelligent security automation
- Collect attack data and developing better metrics to quickly identify threats
- Redefine minimum credentials for entry-level cybersecurity jobs, many of which currently require more than five years of experience and can be a barrier to growing the workforce who is looking to enter the field.

Digital transformation, like any change, brings negatives along with the positives. The cybersecurity challenges are significant but not insurmountable. Though the right technology certainly helps, it s IT security talent that will win the day. Organizations and governments must offer training programs to employees so that they will have the cybersecurity skills needed to defend against tomorrow s complex attacks.

About the Author:

Tom Gilheany is Cisco s Product Manager for Security Training and Certifications. He has a diverse background in startups through multinational Fortune 100 companies. Combining over 20 years of product management and technical marketing positions, and over a dozen years in IT sand Operations, he has conducted nearly 50 product launches in emerging technologies, cybersecurity, and telecommunications. Tom holds a CISSP, an MBA, and is an active board member of the Silicon Valley Product Management Association and Product Camp Silicon Valley.

THE FUTURE OF CYBER SECURITY:
RISK-BASED ATTACK SURFACE VALIDATION AND REMEDIATION



TORSTEN GEORGE

Vice President of Marketing & Products, RiskSense

While malware attacks and data breaches at companies such as Oracle, SWIFT, Cisco, and Yahoo continue to make headlines almost daily, many organizations still practice a traditional approach to enterprise security, which is mainly end point-focused, labor-driven, and vulnerability oriented.

Meanwhile, cyber adversaries have advanced their attack methodologies and long moved on to target new areas of the attack surface, including but not limited to applications, cloud, and Internet of Things (IoT).

In 2017, information security professionals should consider a new approach that assesses the growing attack surface in its entirety and prioritizes remediation based on threat susceptibility and business impact, rather than solely on internal security findings.

This risk-based attack surface validation and remediation process consists of the following five pillars:

1. Attack Surface Coverage

Organizations face an uphill battle when it comes to cyber security, since the attack surface they have to protect has expanded significantly and is expected to balloon even further.

While it was sufficient in the past to focus on network and endpoint protection, nowadays applications, cloud services, mobile devices (e.g., tablets, mobile phones, Bluetooth devices, and smart watches), the Internet of Things (e.g., physical security systems, lights, appliances, as well as heating and air conditioning systems), software-defined networks, microservices, and containers represent a broadly extended attack surface.

According to the Global Risk Management Survey, 84% of cyber-attacks today target the application layer and not network layer, requiring a more holistic approach to cyber security. In turn, organizations need to expand their coverage to include these new areas. This means not only a broader vendor risk management approach, but collection of security data regarding these new attack areas.

"Cyber adversaries have long leveraged machines and automation techniques to streamline their operations. So why shouldn't organizations do the same?"

2. Automation

This wider and deeper attack surface only adds to the existing problem of how to manage the volume, velocity, and complexity of data generated by the myriad of IT and security tools in an organization s network.

The feeds from these disconnected systems must be analyzed, normalized, and remediation efforts prioritized. The more tools, the more difficult the challenge. And the broader the attack surface, the more data to analyze.

Traditionally, this approach required legions of staff to comb through the huge amount of data to connect the dots and find latent threats. These efforts took months, during which time attackers exploited vulnerabilities and extracted data.

Breaking down existing silos and automating traditional security operations tasks with the help of technology has therefore become a force-multiplier for supplementing scarce cyber security operations talent.

Cyber adversaries have long leveraged machines and automation techniques to streamline their operations. So why shouldn t organizations do the same

3. Contextualization

Focusing solely on findings from internal security intelligence such as vulnerability scanners, configuration management databases, and SIEM systems can lead to inaccurate prioritization of remediation actions and inefficient allocation of resources. The POODLE Vulnerability in 2014 is a good example.

The National Vulnerability Database (NVD) originally assigned this vulnerability a 5.5 CVSS score out of 10, which led most organizations not remediate it. Most only act upon security flaws that are rated 7 or higher -- to be able to deal with the onslaught of vulnerabilities in their environment.

However, if organizations had known that hundreds of thousands of POODLE exploits were being carried out, they likely would have changed their risk assessment of the vulnerability.

As we all know, two conditions are required for a security incident to occur: a vulnerability must be present in some form (e.g., a software flaw or insecure programming; insecure configuration of IT infrastructure; insecure business operations; risky behavior by internal staff or other people, conducted maliciously or by mistake) and secondly, a threat must exploit that vulnerability.

"Organizations have tended to focus on known, more visible facts – vulnerabilities and control failures – while neglecting threats as a factor in cyber risk assessments"

Typically, security professionals have no direct control over threats. As a result, organizations have tended to focus on known, more visible facts – vulnerabilities and control failures – while neglecting threats as a factor in cyber risk assessments.

However, as the volume of vulnerabilities has exploded over the past few years, it has become almost impossible to remediate all of them without vetting the impact and likelihood that they will be exploited. The point is, why dedicate resources to fixing vulnerabilities that have no threat associated with them and are not even reachable
Since a threat is the agent that takes advantage of a vulnerability, this relationship must be a key factor in the risk assessment process. It can no longer be treated as risk s neglected step child.

In fact, advanced security operations teams leverage threat intelligence to gather insight into the capabilities, current activities, and plans of potential threat actors (e.g., hackers, organized criminal groups, or state-sponsored attackers) to anticipate current and future threats.

4. Risk-Based Analysis

Once internal security intelligence is contextualized with external threat data (e.g., exploits, malware, threat actors, reputational intelligence), these findings must be correlated with business criticality to determine the real risk of the security gaps and their ultimate impact on the business.

Ultimately, not knowing the impact a coffee server has on the business compared to an email server , makes it virtually impossible to focus remediation efforts on what really matters.

In this context, human-interactive machine learning and advanced algorithms play a big role in driving the proper decision process.

"Using a risk-based cyber security concept as a blueprint, it's possible to implement automated processes for pro-active security incident notification and human-interactive loop intervention"

5. Closed-Loop Remediation

Increasing collaboration between security teams which are responsible for identifying security gaps and IT operations teams which are focused on remediating them, continues to be a challenge for many organizations.

Using a risk-based cyber security concept as a blueprint, it s possible to implement automated processes for pro-active security incident notification and human-interactive loop intervention.

By establishing thresholds and pre-defined rules, organizations can also orchestrate remediation actions to fix security gaps. Meanwhile, cyber risk management provides a way to measure the effectiveness of remediation actions and ensure risks have been successfully eliminated.

"Unfortunately, many organizations close out tickets as soon as a patch is applied without testing whether it actually fixed the problem"

To increase remediation effectiveness, technology-based playbooks that include step-by-step instructions on how to tackle the most critical vulnerabilities can be used.

An intelligence-driven cyber risk management model also mandates a closed-loop remediation process, which assures that a ticket is only closed once the effectiveness of a patch has been revalidated. Unfortunately, many organizations close out tickets as soon as a patch is applied without testing whether it actually fixed the problem.

This leaves them vulnerable to a big blind spot if the patch failed.

Rather than adding more tools, consider implementing these five pillars to establish a new, more efficient enterprise security model.

According to analyst firm Gartner, an approach that uses intelligence-driven analytics can help organizations operationalize cyber security practices, break down silos, and enhance security operations tasks through automation.

About the Author:

Torsten George is Vice President of Marketing and Products at pro-active cyber risk management software vendor RiskSense. Torsten has more than 20 years of global information security experience. He is a frequent speaker on cyber security and risk management strategies worldwide and regularly provides commentary and byline articles for media outlets, covering topics such as data breaches, incident response best practices, and cyber security strategies.

Torsten has held executive level positions with RiskVision (formerly Agiliance), ActivIdentity (now part of HID® Global, an ASSA ABLOY™ Group brand), Digital Link, and Everdream Corporation (now part of Dell).

He holds a Doctorate in Economics and a Diplom-Kaufmann degree, which is comparable to an MBA.

REINVENTING SOFTWARE FORENSICS WITH STATIC ANALYSIS



BILL GRAHAM

Technical Marketing Consultant,
GrammaTech

Introduction:

The term "forensics" refers to the method of using science to discover evidence of criminal activity. Extending this to software broadens the use case to consider all the purposes of software investigation techniques. Software is ubiquitous and part of all major mission-critical systems. As such, software failures have tremendous real world effects. In software, forensics refers to software investigations with tools and techniques that uncover evidence for purposes such as criminal investigations, civil cases (e.g. safety failures), commercial product failures, or security breaches.

Beyond the Law

Investigating software mishaps is important in many industries. Although the required results might not be associated with crime, they are similar to desired evidence gathered during a criminal investigation of software. A prime example would be the investigation of a software failure that has led to an accident resulting in injury, loss of life, or property. Investigators use similar approaches even if criminal activity or negligence isn t suspected.

Software forensics encompasses any activity that requires analysis of source and binary code for investigation, post mortem analysis, or preventive measures. Some examples of use cases for software forensics include (but are not limited to) the following:

- **Malicious code:** A common software forensics scenario would be detecting malicious code and tracking down its author. This code is written on purpose but with hidden intentions. Detection can be difficult with manual techniques, so manual inspections and regular software testing often fail to reveal malicious code.

- **Safety incidents:** Software failures in safety-critical systems have high impact on persons and property. Manufacturers are obliged to track down and investigate the root cause of these problems, either to settle civil suits or to research and prevent future incidents. For example, the FDA used CodeSonar to investigate the quality of various infusion pumps control software, and the NHTSB used CodeSonar to investigate Toyota s unintended vehicle acceleration problems.

- **Security vulnerabilities:** Severe security breaches lead to an investigation into the root of the problem. Security vulnerabilities could be either intentional malicious code or accidental bugs in the software. Root cause and remediation are critical for security vulnerabilities. NIST provides a security incident guide, which provides details on investigation and documentation techniques.

- **Software fault analysis:** In a generic case, any software fault may be the subject of investigation. For example, a monitoring device providing inaccurate results could lead to overcharging a customer (household smart meters, for example). Techniques used to detect and determine the root cause remain the same in this case.

The Role of Static Analysis

Key to many software forensics operations is painstaking manual investigation of source and binary code. Detecting errors or traces of manipulation manually is difficult and time consuming and automated tools and techniques save time and money. To save time and to gain effectiveness, static analysis tools have an important role to play in software forensics.

Malware, for example, is detected by advanced static analysis tools via tainted data analysis from an input source (like a network connection) to where the data is used. If the user is a function with a detected security vulnerability, you have the potential for exploitation. GrammaTech s CodeSonar can also detect security vulnerabilities in binary code, which is imperative when source is not available. Tainted data analysis can also determine if outside input can be used to manipulate a vulnerability into a full-fledged security threat. Automating this process saves huge amounts of manual code analysis. The same kind of

investigation speed up is possible when researching software defects in a software safety incident, for example.

Automated Binary Code Analysis for Software Forensics

Automating something that is otherwise a painstaking and difficult job of manually reverse-engineering binary code, advanced static analysis provides many benefits, including the following:

- **Improved detection:** Automated static analysis can detect errors and vulnerabilities in any size binary executable or library object file, even across multiple compilation units and/or functions. The same analyses by manual approaches are difficult and often limited to pre-determined parts of the binary code. Although automated analysis may not entirely replace manual approaches, it certainly increases the detection rate and scope of analysis.

- **Better tracing:** One of the most difficult aspects of manual forensic investigation is tracing control and data flow, which is exacerbated with binary-only code. Advanced static analysis performs control and data flow analysis on the entire scope of the application. This larger scope of analysis improves detection but also reduces false positives (errors reported that turn out to be false), and aids tainted data analysis. CodeSonar also provides a sophisticated web user interface to significantly help with investigating errors.

- **Investigation efficiency:** Automated vulnerability detection, tracing, and reporting greatly increase the efficiency of binary code investigation. Software forensic investigators can rely on CodeSonar's binary analysis technology to find vulnerabilities in the entire application, while their manual investigation may be focused on certain areas of the code. Considering the cost of manual binary code reverse-engineering and investigation, CodeSonar provides very good return on investment.

- **Reporting to support evidence gathering:** Comprehensive error reporting, code visualization, and integration with vulnerability management systems are crucial to supporting a software security forensic investigation. Automating parts of the investigation-reporting means saving time and reducing errors.

- **Hybrid source and binary analysis:** Although this post has concentrated on binary code analysis, source code analysis is also critical if the source is available. For example, a disgruntled employee may have left malware in source code hiding in plain sight. Source code analysis shares the same features and benefits as binary analysis, and CodeSonar can report on both source and binary results in the same project.

Summary

Software forensics includes the investigation of source and binary code for the detection of not just criminal activity but also malicious code, safety software failures, and security incidents. In most cases, regardless of the motivation for the investigation, the techniques and tools used in software forensics are similar. By increasing the scope, accuracy, and depth of the inspection, CodeSonar saves countless hours of manual binary code reverse-engineering. With clear benefits in terms of security vulnerability detection and evidence gathering, binary analysis is a pivotal tool for software forensics.

About The Author

Bill Graham is a seasoned embedded software development manager with years of development, technical product marketing and product management experience.

Bill can be reached online at @Bill_Graham and at http://iot.williamgraham.ca.

AUTOMATING DATA COLLECTION TO IMPROVE CYBER SECURITY



JAY BOTELHO

Director of Products,
Savvius, Inc.

Data breaches are bad news. We have yet to fully understand the impact of the massive Yahoo breach, which looks like it will go down in the history books as the largest breach to date, but that doesn t mean that smaller and just as damaging breaches aren t taking place every single day. Because they are.

The scale of Yahoo s breach may be unparalleled, but the problems are not. The simple fact is that it takes way too long to discover and resolve breaches. Period. And something has to be done about it.

"According to a report by the SANS Institute, the majority of companies already spend up to 12 percent of their annual IT budget on security"

According to a report by the SANS Institute, the majority of companies already spend up to 12 percent of their annual IT budget on security. The motivating factors span a wide variety of business drivers, including everything from the need to protect sensitive data to regulatory compliance, and a more generic need to improve incident response.

In the past, this traditional security methodology has relied almost exclusively on incremental improvements and updated signatures used in firewalls, intrusion detection and prevention technologies and security information and event management (SIEM) devices. I don t want to sound disparaging about these devices, because they are fantastic at what they do.

But they re not perfect. In recent years hackers have become much better at developing (and sharing) smarter, better targeted and more automated tools that bombard enterprise security systems with a flood of old and new (zero day) attacks. It takes just one chink in the security armor for a hacker to quietly gain access to an enterprise network and sit there undetected for many months while looking around and preparing to exfiltrate valuable data.

Security analysts are overwhelmed

We know that organizations are in a constant arms race with hackers, and we shouldn t expect this to change any time soon. In fact it will probably get worse. The latest IBM and Ponemon 2016 Cost of Data Breach Study found that malicious and criminal attacks took an average of 229 days to discover and an additional 82 days to resolve. Why so long This is a complex issue, but a lot of the blame lies in the fact that security analysts are overwhelmed with data. As more and more alerts are generated by an enterprise s IDS / IPS devices, analysts can only investigate a handful each day.

So what s the solution The simple answer is that security analysts need the tools and the processes to work more efficiently. If we accept the fact that some attacks are going to breach even our best defenses, then the logical step is to improve the way that we respond. In practice, this means two things; being able to discover breaches faster, and being able to resolve them faster. It never ceases to amaze me that companies deploy security solutions to produce all these alerts, but they don t have the bandwidth to analyze them.

"The latest IBM and Ponemon 2016 Cost of Data Breach Study found that malicious and criminal attacks took an average of 229 days to discover and an additional 82 days to resolve"

"Current solutions require a multi-step process where security analysts go to multiple systems for aggregated yet uncorrelated data, then to specific computers for detailed information, and then must correlate all the data manually"

The most logical reasons are that security analysts don t have access to the right data and they cannot access it quickly enough. This is a huge problem. Current solutions require a multi-step process where security analysts go to multiple systems for aggregated yet uncorrelated data, then to specific computers for detailed information, and then must correlate all the data manually.

The very best data is in the network packets, but none of it is indexed to the alert, and access to such data is typically a network function, not a security function. And if the alert is older than a few days then the original packet data have probably been discarded. Security engineers need access to all of the packets related to an alert right at their fingertips, at the click of a button.

As alerts are received from a security system, a computer should parse them, storing the network packet data that correlates with the source of the alert. Packet data related to IP addresses and log data from a SIEM can be pulled together in the background, making it easier for an analyst to access the data with a single click to evaluate whether an issue needs further investigation. If they see, for example, that log and packet data don t match, then a deeper look is warranted.

Centralize and automate data collection, and make it searchable.

Automating alert-related data collection will allow that data to be stored in a central location, but that one place doesn t exist yet.

Currently, analysts typically go to something like a SIEM dashboard, log into a host machine or other UI, switching between multiple software applications or devices to access information. This is ridiculously time consuming and inefficient.

The security industry needs to develop automated processes that automatically collect relevant suspicous packet data and make it readily available for analsyts. This will make their jobs more efficient, while helping them investigate more alerts each day. If that can happen, I think it s reasonable to expect analysts productivity to increase signifcantly.

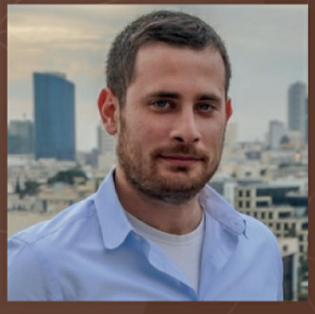
About The Author

Jay Botelho is the director of products at Savvius, Inc. a leader in packet intelligence solutions for network performance management and security investigations. Jay holds an MSEE, and is an industry veteran with more than 25 years of experience in product management, product marketing, program management and complex analysis.

From the first mobile computers developed by GRiD Systems to modern day network infrastructure systems, Jay has been instrumental in setting corporate direction and specifying requirements for industry-leading hardware and software products. He is based at Savvius headquarters in Walnut Creek, California.

Jay can be reached online at JBotelho@savvius.com or @jaybotelho, and at the company website: http://www.savvius.com/

THE CURRENT STATE OF ICS CYBER SECURITY



BARAK PERELMAN

CEO,
Indegy

The emergence of new cyber-threats targeting ICS networks, combined with trends like IoT and connected industry, is forcing the industrial sector and governments to take a long, hard look at the way they protect these networks.

After all, the consequences of a successful attack can go far beyond financial and reputational damage to the organization. It can have implications on physical processes, the surrounding environment, and even human lives.

> *"Chiefly due to lack of built-in security mechanisms like authentication or encryption, the absence of event logs and the fact these networks operate differently than IT networks"*

Compared to IT networks, ICS networks pose very different security challenges. Chiefly due to lack of built-in security mechanisms like authentication or encryption, the absence of event logs and the fact these networks operate differently than IT networks.

Most ICS networks were designed and implemented before the Internet, when hacking and cyberterrorism did not exist.

Therefore security was not accounted for. Furthermore, since these networks were behind an air-gap, many legacy systems are still in place, unpatched and vulnerable.

This makes ICS networks an easy and attractive target. Freelance terrorists, state-sponsored groups, hacktivists, professional criminals, and disgruntled employees are the usual suspects for attacks.

Internal and External Threats to ICS Networks

ICS networks are prey to numerous threats. Some of these threats can come from external sources, some are posed by malicious insiders, but in many cases, the biggest fear is from plain old human error.

External Actors

External cyber attacks targeting ICS networks often originate from politically motivated adversaries (a nation state, terrorist group, or hacktivists). However, industrial espionage from industry competitors is quite prevalent also.

In recent years the world has experienced a number of ICS cyber attacks, including the attack on the Ukrainian power grid, the German Steel Mill Cyber Attack, and others. But most security experts suspect that the vast majority of ICS hacking incidents go unreported for reasons of security, or to avoid embarrassment.

It is important to note that an organization doesn t need to be the intended target to suffer the consequences of an attack. Once malware is out in the wild, it is very difficult to limit its activity and control its impact.

The Best known example is Stuxnet: a sophisticated computer virus that is claimed to have been designed to attack Iran's nuclear-enrichment facilities in Natanz.

It also infected Chevron Corp.'s network in 2010, shortly after it leaked from its intended target. According to Mark Koelmel, general manager of the earth-sciences department at Chevron, Stuxnet was only discovered in the company s systems after its existence was reported in the news.

It is likely that those who designed the virus also weren t aware how far it had spread.

Internal Threats

Insiders with access to ICS networks include employees, contractors, and third party integrators.

Since most ICS networks don t have any authentication or encryption mechanisms that restrict user activity, any insider has unfettered access to any device in these networks.

This includes SCADA applications and the critical controllers responsible for the entire lifecycle of industrial processes.

A well-documented example of an insider threat is the case of Vitek Boden, a man who worked for Hunter Watertech, an Australian firm that installed SCADA radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia.

After installing the equipment, Boden applied for a job with the council, which decided not to hire him. He retaliated by using (possibly stolen) equipment to issue unauthorized commands that caused 800,000 liters of raw sewage to spill into local parks, rivers, and residential areas, causing extensive environmental damage.

"Some errors arise when employees use 'creative measures' to get their work done faster — such as remotely connecting to the ICS network even though they lack secure access."

Human Error

Human error can range from employees or third-party integrators performing maintenance work within ICS networks. Setting incorrect configurations on control devices (PLCs, RTUs, DCSs) can cause a wide range of disruptions. In some instances planned work was not fully executed or not executed at all.

Some errors arise when employees use creative measures to get their work done faster — such as remotely connecting to the ICS network even though they lack secure access.

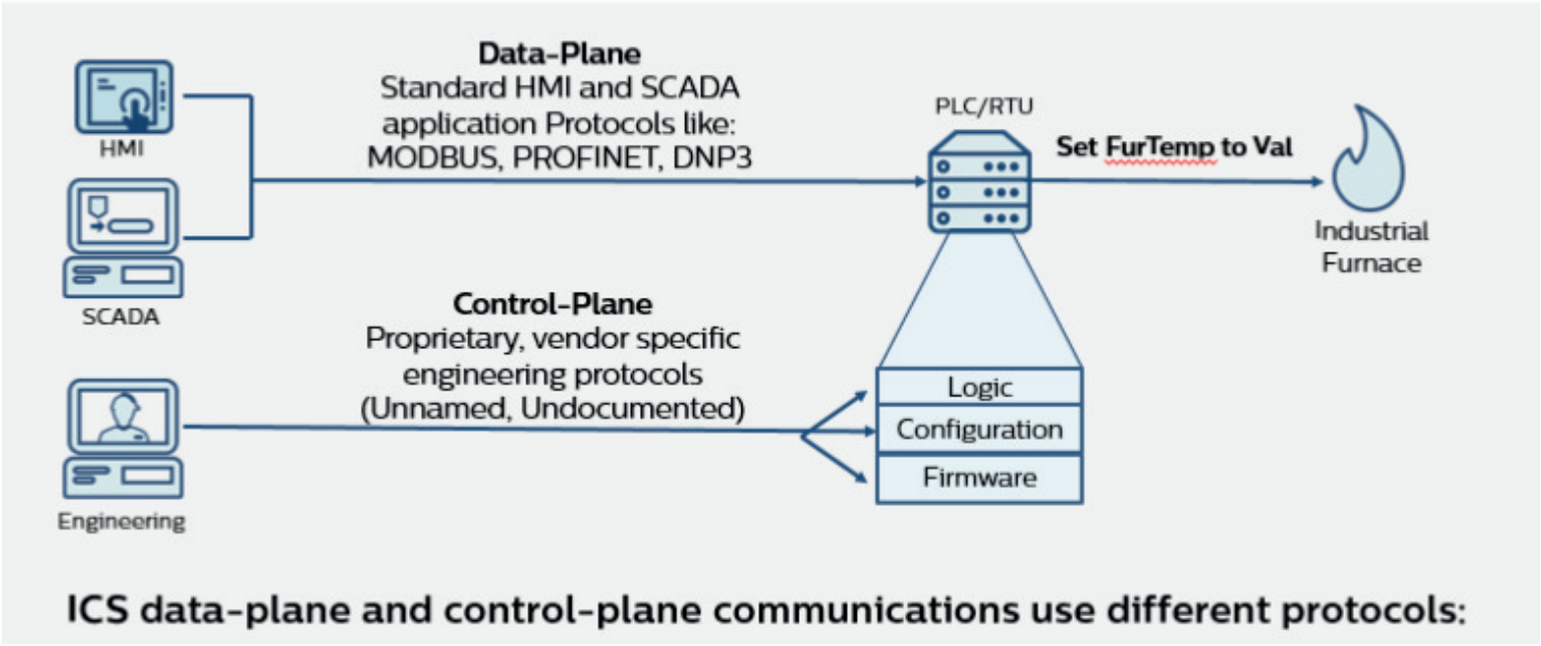
In other cases, integrators set up an external connection to enable access for the duration of the project, and leave it behind when the project has ended. These unsanctioned connections can become infiltration points that expose the network to external attacks.

Without any logs to track these activities, it becomes very difficult to identify the source of problems, discover who/what caused them and what should be done to mitigate problems. As a result, industrial organizations are often required to invest significant amounts of time and resources to investigate disruptions that could have been avoided to begin with.

The Most Critical Assets: The Automation Controllers

The brains of all ICS/SCADA systems are the automation controllers like PLCs, RTUs and DCSs, which automate industrial processes and manage equipment like turbines, pumps, valves and more.

These controllers are not just proxies in the network. They are specialized industrial computers that make logic-based decisions and ensure continuous operations.



ICS data-plane and control-plane communications use different protocols:

They apply safety thresholds to prevent dangerous settings and manage the entire lifecycle of industrial processes. In fact, in a properly designed system, even if the operator station (HMI or SCADA interface) is not available, the controllers will make sure the process continues to operate as planned.

This means that any changes to automation controllers can have significant impact of the safety and continuous operations on industrial processes. Therefore these type of changes must be closely controlled and logged. However, as mentioned earlier, there are no built-in security controls in place, and no event logging exists to keep track of such activities.

"The lack of a comprehensive audit trail, or event log, detailing changes to controllers makes it very difficult to determine if operational disruptions were caused by a cyber-attack, a malicious insider, human error, or mechanical failure"

The lack of a comprehensive audit trail, or event log, detailing changes to controllers makes it very difficult to determine if operational disruptions were caused by a cyber-attack, a malicious insider, human error, or mechanical failure.

This lack of visibility and controls limits the ability of operations staff to respond to events in a timely manner, raising the overall costs of disruptions and mitigation efforts.

ICS Network Security Challenges

ICS networks are inherently different than IT networks. Not just because they use unique protocols, specific to OT networks, but also because different activities are carried over different protocols - a dichotomy that does not exist in IT networks:

Data-Plane Activities, e.g. process parameters, registers, are communicated via HMI and SCADA applications over standardized and well known

industrial protocols like MODBUS, PROFINET and DNP3.

Control-Plane Activities, e.g. all changes to the controller devices, including configurations, firmware uploads/downloads, code updates are executed over different protocols which are proprietary and vendor-specific.

This is due to the fact that each OT vendor has developed their own proprietary engineering software and protocols for these tools.

These protocols are largely unnamed and undocumented because when they were developed vendors assumed that changes to controllers would only be made via their software tools.

Over the years, additional tools that utilize the protocols have been developed, mostly for research purposes. Adversaries are also familiar with these protocols and the activities that can be executed using them.

The fact that there are no restrictions over the use of control-plane protocols, and no logging, makes them a very attractive attack vector. It also enables adversaries to cause significant damage while remaining undetected.

In an IT network, this would be akin to allowing anyone with network access to execute privileged activities on critical assets. This, of course, is a completely unacceptable practice.

"It is vital to track all access and changes to automation controllers, not just to identify malicious activities, but also for discovering issues caused by human error"

Keys to Securing ICS Networks

Implementing security controls in ICS networks is not easily resolved. The first step requires gaining real-time visibility into all the activities on the network.

It is vital to track all access and changes to automation controllers, not just to identify malicious activities, but also for discovering issues caused by human error.

Only with full visibility into the control-plane can organizations apply effective security and access management policies that govern who is allowed to make what changes, when and how.

New, specialized monitoring and control technologies designed specifically for ICS networks can provide the deep, real-time visibility required to identify suspicious or malicious activity, and to take preventative action to limit or stop damage.

Real-time monitoring of control-plane activities, namely the engineering changes made to industrial controllers either over the network or on devices is the most effective way to detect unauthorized activities and minimize operational disruptions.

About the Author

Barak Perelman is CEO of **Indegy**, an industrial cyber-security firm that improves operational safety and reliability for industrial control networks by providing situational awareness and real-time security.

THE MIRAGE OF DATA SECURITY COMPLIANCE AND THE FEDERAL TRADE COMMISSION



MICHAEL DAUGHERTY

Cyber Security &
Regulatory Compliance Expert

To get one step ahead of a regulator, you need to know which could impact your business and what laws, rulings or actions they have recently taken to affect your kind of business, here in America. In my case, at LabMD, dealing with cancer screening, I would have thought Departement of Health and Human Services (HHS.gov) on the HIPAA/Hitech act would have been the one to watch out for but some regulators are out of control and until it stops, all small to medium size enterprises (SMEs) in America need to heed my warning and understand my case against the Federal Trade Commission (FTC.gov)

For those living under a rock, the Federal Trade Commission has anointed itself Chief CyberCop. They ve done this, they argue, because Congress gave them this authority in 1914, when FTC was created. In its current form, the **act** states that "unfair methods of competition ... and unfair or deceptive **acts** or practices in or affecting commerce, are hereby declared unlawful." The FTC has taken those words and stretched more than taffy was ever known to stretch.

They re all dead now, but I doubt 1914 lawmakers knew the internet was coming. The FTC act was not designed for today's world. Yet agencies assume power arbitrarily and only relinquish power when ordered by the courts or Congress. But challenging an agency's self-appointed power takes years and millions.

This takes time and money few have to spend while your reputation is shredded as everyone assumes you're guilty. And don t think these bureaucrats don t know it. They expect cowardly companies to write a check, agree to terms, and run out of Washington with their hair on fire. This is how it is, but it is not how it was supposed to be.

Over a century ago, at the beginning of the medical and industrial revolution, administrative agencies were born. Created because they were supposed to be "experts", which is a noble idea, but over the decades the experts have been replaced by government lawyers with no detailed knowledge of how systems work, trying to enforce cyber issues they little understand. This is a recipe for disaster and the disaster is here.

On the cybersecurity side, the FTC has ruled that it is a violation of law and an unfair trade practice to have a hackable system. Specifically, a breach isn t required. Data only needs to be exposed or vulnerable. Read that again…only exposed or vulnerable. (and they won t define those terms)

The FTC will not publish standards. This is practicing secret law. They actually fight to keep standards secret. This is outrageous as all systems are hackable. Therefore, all companies with hackable systems have committed an FTC Section violation. How much money will it cost to achieve the unachievable Compliance has been made impossible and transformed into a game of roulette. Try explaining that to your C-Suite as they look for heads to roll after an incident.

On the practical side, arbitrarily enforcing the impossible against persons with hackable systems detracts from the main focus that should be on everyone's mind -- how do we determine how to protect information that should be protected, and how do we regulate in this area so that we can truly protect our property and privacy

"The fact that the Federal Trade Commission chooses to ignore reality and attack victims of hacks instead of the hackers themselves is counterproductive and damaging"

The fact that the Federal Trade Commission chooses to ignore reality and attack victims of hacks instead of the hackers themselves is counterproductive and damaging. Law firm client alerts perpetuate this atrocity by lulling clients into believing that there is some rationality behind FTC policy. What there really is is money to be made assisting you to navigate this maze of government deception. This will not stand the test of logic or, we hope, real judicial review. But this is really all about power, not justice or security. Until Congress untangles itself and requires real published standards developed with input from the tech industry, cross your fingers that the knock on your door isn t from the FTC. If they show up, you re already guilty unless your security is perfect.

Since the odds of the FTC knocking on your door are very slim you may be lulled into thinking this isn't your problem. But that's exactly how they get to you. They get to you by holding up the companies they bully into settling so you ll observe what got that company into trouble. You ll make sure you re not doing that specific bad thing. You will spend money and time, train more employees, and invest in more equipment chasing the illusion of compliance. And under the current regime at the Federal Trade Commission compliance is exactly that…an illusion.

"Because you actually are in Las Vegas when dealing with the FTC and they are the Casino. Remember, the house always wins"

But, since the FTC ensnares so "few", "the many" don't seem to care much. Until the tech world demands regulatory involvement as the healthcare world did in developing HIPAA, you ll just have to pretend you're in Las Vegas, roll the dice, and take your chances. Because you actually are in Las Vegas when dealing with the FTC and they are the Casino. Remember, the house always wins.

We need to get not only one step ahead of the cyber criminals, some of which in my case, were employed in their reckless actions and attempted cyber blackmail with the support of the FTC. While you may say this runs counter to all common decency and common law, causing a great company with great people on a humane mission, LabMD, to be another victim of government overreach and misbehavior, the bottom line is this – they own the bulldozer, we paid for it with our taxes and they will use it to run over you without a humane thought in their minds. The old expression just doing my job is no excuse for government overreach and the way it harms SMEs in our great Nation. We, together, must not stand for this any longer.

"The old expression "just doing my job" is no excuse for government overreach and the way it harms SMEs in our great Nation. We, together, must not stand for this any longer"

My words of Widsom to anyone in INFOSEC who cares about their job and their company…

I ve finally had an epiphany, even though we hear about the battle to stop terrorists means the NSA and the CIA want backdoors in everything Again, government agencies run afoul of their missions which cannot circumvent the US Constitution, ever, without their activities being illegal and unconstitutional. FTC, NSA, CIA, FBI, all these three letter agencies want more power

and more control over all of us because they think they know better than those whom they serve.

> *"The only way to fight back, seeing as Congress hasn't been able to protect our rights, is to promote, use, share, train others in STRONG ENCRYPTION, ANTI-PHISHING, and BREACH PREVENTION"*

The only way to fight back, seeing as Congress hasn t been able to protect our rights, is to promote, use, share, train others in STRONG ENCRYPTION, ANTI-PHISHING, and BREACH PREVENTION. We must encrypt the PII and have proper key management. We must begin to consider getting one step ahead of the next Spear Phishing attack, Remote Access Trojan (RAT) and Ransomware. Breach Prevention solutions like that from SnoopWall, a company of which I serve on the Board of Directors are designed to be affordable and cost effective in helping SME s get one leg up on the next wave of cyber attacks.

And who would have ever thought a wave of criminal cyber attack activity could be condoned by a government agency like the FTC.

Well, now you know. Millions of dollars in legal fees later and countless hours standing for what is RIGHT and what is JUST, I share with you my pain so that you never have to suffer in this way. Don t say I didn t warn you.

Learn more about this incredible story of 3 letter agency overreach at http://michaeljdaugherty.com/ and stop by Cyber Defense Magazine s press room where I ll be at various times during the RSA Conference USA 2017 to discuss in more detail and for book signings.

About The Author

Michael Daugherty is a Cyber Security and Regulatory Compliance Expert. He frequently writes for Cyber Defense Magazine and was the President & CEO of LabMD, an Atlanta-based clinical and anatomic medical laboratory with a national client base until the FTC destroyed it. LabMD specialized in analysis and diagnosis of blood, urine, and tissue specimens for cancers, micro-organisms and tumor markers.

Mike founded LabMD in 1996 after 14 years in surgical device sales with U.S. Surgical Corp. and Mentor Corporation. Outside of his case of LabMD vs FTC, Michael enjoys serving on advisory boards, is on the Board of Directors of SnoopWall, among others.

He enjoys playing tennis, traveling, and flying his Cirrus SR22 Turbo single engine aircraft. He is a member of the University of Michigan Alumni Association, the Atlanta Aero Club, and the Cirrus Owners and Pilots Association. Born and raised in Detroit, Michigan, Mike holds a BA in Economics from the University of Michigan-Ann Arbor, and has resided in Atlanta since 1987, when he moved to Atlanta from Portland, Oregon.

Mike can be found at: http://michaeljdaugherty.com/ and

Facebook: http://www.facebook.com/daughertymichaelj
Twitter: https://twitter.com/daughertymj
LinkedIn: http://www.linkedin.com/pub/michael-j-daugherty/19/8/7a5
Google+:
https://plus.google.com/u/0/118277419398075017990/posts

STARTUPS WITH INFORMATION SECURITY IN MIND AT STARTUP

WHAT'S THIS ALL ABOUT AND DOES IT REALLY MATTER?



KIP

Cyber Security Expert

There are some very talented people starting company s solving very complex problems that can save organizations millions of dollars. From providing security services, IoT, GIS solutions, auditing of systems, and SaaS platforms which provide elastic environments allowing companies to use a service that can surge when the demand is there and shrink when demand is low saving more money.

My recent research of startups early stage companies, I found one key commonality that should NOT be there – a lack of forethought and planning of information security; in particular an INFOSEC program that would protect the environment, the startup crown jewels so to speak, from current cybercrime and malware threats.

When I asked C level executives at many of these companies about this deficiency, the common answer I received is it was too expensive or there is no time to implement security.

Lets take a step back and look at that statement a bit, what is at risk The information is startup proprietary information, potential patent information, potential personal identifiable information and customer information. On an average of the startups and established company that I have interactions there was very little or any commitment to information security within the products or services that were provided.

My key discovery was that there is a threshold of when the companies would start to think of security. The time was when a potential customer would require the necessary steps to require the security of their information that has been provided. This is an afterthought – where, for example, has the information been stored, processed or shared. In the CISO arena, it boggles the mind to think most startups are not even thinking they will be victimized – hence many SME s (small to medium size enterprises) face their demise now, more from a cyber attack, than lack of early stage revenues.

In fact, most SME s cannot suffer a single breach without going out of business, due to the very high costs of remediation, regulatory compliance related issues, fines, brand damage and loss of customer confidence.

If you look at US law and UK data protection of personal information there are a number similarities as there are specific requirements to protect personal information. Specifically the US requires an opt out while an opt in for the UK for all marketing events.

Where is your information with services that you have provided some of your personal information

This is not the responsibility of the customer but the responsibility of the companies that would use the services of a startup or a well-established organization.

How do we address security in a cost effective method that would protect everyone

Below is a list of an example of tools that can be used at either zero cost for the use or marginal cost as it relates to the customer privacy. There is

CIS who provide security hardening guides for free
https://benchmarks.cisecurity.org/downloads/benchmarks/

AWS provides free AMI s that are hardened to CIS standards
https://aws.amazon.com/marketplace/pp/B00UVT5ZIW

AWS S3 encryption at rest
https://aws.amazon.com/blogs/aws/new-amazon-s3-server-side-encryption/

Insecure.org provided a number of the best rated security tools that are available
http://sectools.org/

WAF for AWS
https://www.howtoforge.com/tutorial/install-nginx-with-mod_security-on-ubuntu-15-04/#-download-modsecurity-and-nginx

These are just examples of tools that can use to secure software and infrastructures and meet the technical controls. The question leads to why there a number of investors out there willing to invest in an organization that has not considered if the organization has included security

In fact, some startups get acquired, just like the bigger player, Yahoo , only for the acquirer to find out they ve already been victimized in cyber crime – whether it be repeated ransomware attacks or a complete data breach of all the customer personally identifiable information (PII).

This either leads to shareholder lawsuits or an incredible reduction in the final acquisition cost payout.

Lets consider the impact of not protecting information; legal proceeding can lead to closing the doors of an organization, further compensation to the injured parties or affecting the reputation of an organization.

What are some simple steps to include security into a new company to be cost effective.

1. Understand the sensitivity of the information you are handling
2. Understand the legal liability in the event of a data slip
3. Treat the information you receive, as it was your won
4. Encrypt all data from the start unless you are processing the information which would require the information to be unencrypted
5. Keep the system up to date to close security vulnerabilities in Operating systems and software used to deliver the service.
6. Review all developed code for potential vulnerabilities
7. Always prepare for a disaster. Create a plan of action if a severe data breach takes place. Your reaction will make the difference in legal ramifications and corporate reputation.
8. Train personnel in the handling of sensitive information

For Investors and those that are thinking of starting a company providing services, think about security upfront rather than an after thought. It is more expensive to not include security at the beginning of your product than after a request from a potential customer or a compromise.

When you start the adventure of a new business, think of the information you handle to be your own and how would it make you feel if your information was stolen.

About the Author

Kip has served as a CISO for the past 8 years and IT Executive leader for over 20 years. He uses extensive business and security expertise to advise CXO executives on strategies to deal with quickly changing landscape that affecting IT infrastructures. His current focus is on International Privacy Laws, compliance to ISO, SSAE 16, HIPAA, in technology mobility, advanced malware, APT, and cloud security.

Kip brings over three decades of IT security leadership spanning the military and commercial experience. He previously served as a US Marine in Information Technology and a CISO at United Launch Alliance, GeoEye and ServiceSource. He has specialized in building Risk Programs, IT Departments and Security programs.

AMAZON'S ECHO MAY BE SENDING ITS SOUND WAVES INTO THE COURT ROOM AS OUR FIRST "SMART WITNESS"



ANDREW L. ROSSOW, ESQ.

Cyberspace Attorney,
Gregory M. Gantt Co. L.P.A.

Cyber-Space and Technology Attorney, Andrew Rossow, discusses the current law enforcement investigation involving the murder of Victor Collins, back on November 22, 2015, and a potential smart witness, which just so happens to be Amazon's Echo smart device.

"Hey Alexa, will anything I say to you be used against me in a court of law?"
"I'm sorry, I cannot answer that question at this time"

Today, consumers are engulfed in the world of smart devices. As of the 2016 holidays, the most purchased gift for the season was Amazon s Echo, a smart-device that the consumer can speak to back and forth to control other smart devices, stream music and audio, and receive updates on news, sports, and weather.

But, what happens when that smart device has the potential to be used against you in court….for EVERYTHING you say and EVERYTHING it hears Welcome to the a new age of rules and policy that the courts and rules of evidence will soon have to address…a lot sooner than you think by the look of things.

A. WHAT IN CYBERSPACE IS "ALEXA"?

Amazon s Echo , dubbed Alexa out of three possible names (Amazon, Echo, Alexa), is a cylindrical, spherical (Echo and Dot) smart voice-enabled speaker that allows for a user to connect wireless and Bluetooth devices to it; receive news and weather updates; stream music and video libraries; and connect to third party services such as Calendars and e-mail providers. The device is equipped with seven microphones and responds to a wake word—Alexa or Echo, most commonly. When it detects its wake word, it begins streaming/recording audio to the cloud.

Amazon has found itself at the heart of a murder investigation, dating back to the night of November 22, 2015. James Bates called Arkansas police that night stating him and a few work buddies, including the victim, Victor Collins, had stayed up the night before watching football with some drinks. Mr. Bates told authorities that he had let two of them stay at his place to crash and after waking up the next morning, found Collins lifeless body in his hot tub. After further investigation, police suspected foul play after finding broken bottles and blood spots around the hot tub. Inside the house, authorities found a plethora of smart home devices including a Nest thermometer, a Honeywell alarm system, and an Amazon Echo. Upon this finding, police believe there could be some pertinent information on Amazon s servers, in the event one of the individual s that night inadvertently woke Alexa up and it recorded conversation(s). The Bentonville Police Department seized the Echo, which was on Bates countertop and served what allegedly is claimed to be an overbroad warrant of any and all audio records the Echo may contain. In response, Amazon has declined to provide any information, as it claims the warrant is too overbroad. While police have been able to extract some information from it, the goldmine (if anything), lies in Amazon s servers.

As of recent, Amazon s Echo has been the primary subject of a murder investigation dating back to November 22, 2015….ironically, it could be a HUGE WITNESS to the investigation, if it s allowed to testify that is. Yes, you heard me correctly.

The Fourth Amendment to the United States Constitution provides the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In this investigation, there are several questions pertaining to the 4th Amendment that present themselves. First, an individual must have standing to claim protection under the 4th Amendment. To have standing, there must be a reasonable expectation of privacy, which contains both an objective standpoint and a subjective standpoint. To answer this question, we must follow up with a second, but

more complex question: When it comes to smart devices, such as the Amazon Echo, is there a difference in the reasonable expectation of privacy one may have Better yet, should there be a difference While I am not fit to answer this on behalf of all of us, the most promising answer is the one lawyers know best…it depends. These smart devices do an EXCELLENT job of informing us that they used cloud based services to connect and store our data. This is how these devices are able to link or connect to our music libraries, phones, calendars, notes, ect. However, while we give these devices permission to connect our accounts, we also don t like other people (law enforcement, users, businesses) having the ability to connect to our devices or extract information from our devices whenever they want. Otherwise, why would we purchase something like this I guess my answer would be, YES THERE IS A REASONABLE EXPECTATION OF PRIVACY that society deems exists with these devices, but at the same time, depending on where the device is placed, how it is used, and why it is being used, determines how far that expectation goes. This continues to be an open-ended question.

Second, in the event there is standing for a person to challenge an issue against the 4th Amendment, we can look at the right of a person to be secure in their home against unreasonable searches and seizures. The last thing any of us expects is to have to worry about what we do in our own homes. While we know Alexa listens for its wake word, the last thing we d expect is when we bring it home, worrying about her ratting our every move out to law enforcement, albeit legal or not. This is troubling to say the least. Alexa is supposed to IMPROVE and ADVANCE our home, not make it VULNERABLE or the subject of any sort of legal investigation.

Third, the right of a person to be secure in their effects against unreasonable searches and seizures. While our Framers never included a definition to the term effects in the Constitution, courts have still applied the reasonable expectation of privacy standard to personal property. When an individual s personal property is not inside their home or on their person, there is little to no protection . Alexa is considered personal property within personal property. In a sense, Alexa is a storage device for other personal information we give it access to such as our calendar, notes, reminders, and other personal information. It s only logical that whatever information of ours that Alexa has been given permission to access or link to, that it also be protected.

Lastly, that no warrant shall be issued except on probable cause, describing the place to be searched and persons or things to be seized. This requires a warrant specifically and particularly identify the places and persons to be searched, and things to be seized. A warrant will be held invalid if it is too broad or requests general items. We all know searches and seizures are illegal without a warrant. In order for law enforcement to obtain a search warrant, there must be probable cause shown to the Magistrate. Probable cause is where there is a reasonable suspicion that a crime is being committed, about to be committed, or has been committed. While there are exceptions to the warrant requirement (not discussed here), none address smart devices, obviously.

Looking into the pending investigation, Arkansas law enforcement officials recently issued a warrant for Amazon to release any and all recordings from its Alexa device that night, owned by Mr. Bates. In response, Amazon declined to release such information and stated the following to Engadget : "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."

B. NEW DEVICES, SAME LAW….RIGHT?

Currently, our legal system is finding ways to FORCE smart technology into the rules of civil and criminal procedure (both statewide and federally). Realistically though, it s the same law being applied or forcibly applied to include these new devices. However, the obstacle and the opinion of many in the field is that our laws are outdated when it

comes to smart technology in terms of how Courts address it on an evidentiary level.

So, the first question is, how can smart devices be used in court If it can be, which we are starting to see and learn more about, when can they be used in court Technically, these devices do produce statements and are advanced enough that it could be considered a person for all intents and purposes. Indeed, that is an entirely different discussion for another time.

Under the Federal Rules of Evidence (Rules) evidence is relevant if it has any tendency to make a fact more or less probable than it would be without the evidence and the fact is of consequence in determining the action. Additionally, all relevant evidence is admissible unless…another Rule says otherwise . Specifically, statements that are considered hearsay are not admissible unless an exception applies. Hearsay is any statement made outside the presence of court by a person for the purpose of offering it to prove the truth of the matter asserted.

In the pending investigation of Mr. Bates, if the recorded audio were to be extracted and given to the Prosecution, these recorded statements are considered hearsay because it was made by Amazon s device outside of court, for the purpose of corroborating or proving that Mr. Bates either did or did not commit the murder of Mr. Collin s. Currently, there is no hearsay exception that would allow for statements by Alexa to come into evidence as admissible. This is a problem where we are in an age of smart devices that we are constantly communicating with to advance our lifestyles. But that s just it…isn t it A smart device…communicating Sounds like testimony to me, just as accurate as if the person themselves were testifying, no

Indeed, it would make sense for experts and the writers of the Rules to consider amending them to include provisions that address smart technology, whether it is adding a hearsay exception or other such appropriate provisions. This is a long process though and many more cases would need to be brought before the court before any such legislation is considered. With cases like this and the San Bernardino case involving the FBI s request for access into an individual s iPhone, you can most certainly count on hearing more about the court s involvement in these matters.

We will continue to see unique cases like this become more common, as augmented reality and virtual reality is attempting to establish its presence in our market. It is only a matter of time, sooner rather than later, that courts will have to make rulings on the impact our technology has and will have on our laws and court system.

Until then, Mr. Bates next court hearing is March 17th, 2017. I agree with Marc Rotenberg, the president of the Electronic Privacy Information Center, in his recent statement that there needs to be a clear legal standard that governs law enforcement access to these smart devices. These smart devices certainly open the door to warranted privacy concerns on many levels. It will be interesting to see what measures are taken to address privacy concerns and evidentiary concerns in the course of this investigation.

About The Author

Andrew Rossow is a Cyberspace and Technology Attorney at Gregory M. Gantt Co. LPA in Dayton, Ohio. He graduated from Hofstra University School of Business in New York and received his J.D. from The University of Dayton School of Law. He practice focuses on Cyberspace Law & Internet Law, Intellectual Property Law, Entertainment Law, Criminal Defense, Contract Disputes, and Probate.

Andrew can be reached online at drew@ganttlaw.com or follow him on FACEBOOK at facebook.com/drossowlaw and TWITTER at @drossowlaw, and at our company website http://dayton-lawyers.net/attorneys/andrew-l-rossow.html

RUNTIME APPLICATION SELF-PROTECTION (RASP) - THE FUTURE OF APPLICATION SECURITY



JOHN MATTHEW HOLT

Founder & Chief Technology Officer,
Waratek

Applications are the collective blind spot of cyber security because organizations typically devote most of their security resources to protecting their perimeters.

Meanwhile, traditional approaches for securing applications have come up short. These include writing more secure software code; and installing Web Application Firewalls (WAF). Both are extremely labor-intensive, costly, and largely ineffective.

"Not only does it address the deficiencies of the above security approaches, but it introduces new capabilities that represent a paradigm shift in the way enterprises secure their data and applications."

Enter RASP, a relatively new model for application security. Not only does it address the deficiencies of the above security approaches, but it introduces new capabilities that represent a paradigm shift in the way enterprises secure their data and applications.

The core idea of RASP is that the runtime of an application contains all the data and context required to prevent the execution of tainted code.

In other words, the application runtime affords full contextual awareness.

This enables RASP to detect and mitigate most common forms of cyber-attack such as Command Injection, Cross Site Scripting, and SQL Injection with precision, avoiding false positives and false negatives.

Since its emergence in 2012, RASP has been growing steadily due to the influx of quite a few vendors and the proven strength of the technology, which is popular in the banking and financial sector across Europe and the United States.

First Generation Application Security Isn't Working

With the number of applications and the volume of known vulnerabilities multiplying at alarming rates, writing better code is a losing proposition.

As for WAFs, they are costly to purchase, difficult to operate, and generate a high level of false positives that must be investigated.

A 2014 NSS Labs report comparing popular WAFs found the average Total Cost of Ownership exceeded $5 per connections per second, and produced an average false positive rate of .77%. That translates into millions of false positives per month for a high-transaction, high-volume organization, and significant labor cost / lost productivity associated with the resulting investigation.

"An average of 395 hours is wasted each week detecting and containing malware because of false positives and/or false negatives"

Meanwhile, a 2015 report from the Ponemon Institute estimated that an average of 395 hours is wasted each week detecting and containing malware because of false positives and/or false negatives.

Oracle, Microsoft, other software developers, and the security community routinely report serious flaws (an average of one every 100 hours in the case of Oracle s Java),

prompting immediate action to install critical updates. Each new update starts a race between attackers and defenders: can the patch be applied before an attack occurs exploiting the publicized weakness

It takes, on average, three to six days for an attacker to successfully exploit a vulnerability, more than 250 days to discover an attack is underway, and an additional 82 days to contain the attack, noted the Ponemon Institute in its 2015 Cost of Data Breach Study: Global Analysis.

The constraints of limited manpower and stressed budgets are compounded by the risks of reopening old source code, where the original developers are gone and documentation may not be up-to-date or accurate.

RASP: Instrumentation or Virtualization

There are several flavors, or implementations, of RASP. One requires specific sections of code be instrumented to enable RASP. Routinely, instrumentation results in changes to application artifacts such as source code, deployment descriptors, or binaries to allow highly targeted use of RASP.

Instrumentation involves recompilation or redeployment of an application, and will result in operational intervention when the RASP configuration is first introduced or subsequently changed.

Another approach, container-based RASP (also referred to as RASP by virtualization) applies security at the container level, using rules to govern how RASP protects the application. This approach completely eliminates the need to make changes to application artifacts, and has no impact on the application lifecycle or its normal operations.

Three Benefits of RASP

Precision Application Protection

This refers to RASP s ability to eliminate false positives and false negatives by enforcing security within the application or the application container — thus giving it access to all application and user data as well as the context needed to differentiate between the two.

The instrumentation approach is more granular than the containerized one. It gives developers complete control over which lines of code will be RASP-enabled, allowing them to strike a balance between protection and performance.

The trade-offs of instrumentation are significant costs in terms of developer time and financial expense.

Containerized RASP provides fine-grained precision of the container rather than the code. Containerized RASP requires no direct interaction with the application code, no prior knowledge of the application, and involves no recompilation step. This more automated approach results in significantly lower costs, without any performance impacts.

"This more automated approach results in significantly lower costs, without any performance impacts."

Virtual Patching

Through 2020, 99 percent of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least a year, predicts Gartner.

Understandably, keeping up-to-date with the latest patches has become a major concern for enterprises and a significant challenge for every CISO.

Complicating matters are: the shortening time between the emergence of exploits, and the sheer number of new

vulnerabilities. This increases the pressure on IT managers to rapidly patch production systems —pitting the need for rapid response in conflict with the best practices of quality assurance testing.

Zero Day Vulnerabilities are another cause of disturbance to planned application patching and release schedules, diverting yet more resources from application development to patching.

Many organizations struggle to keep on top of an avalanche of new patches and updates. At the same time, they are forced to maintain 100-percent availability of critical business systems.

> *"Using RASP's virtual patching capability, organizations can mitigate both routine and emergency security vulnerabilities without the need to install patches, change code or incur any downtime"*

Using RASP s virtual patching capability, organizations can mitigate both routine and emergency security vulnerabilities without the need to install patches, change code or incur any downtime.

This is especially valuable for shortening attackers window of opportunity between when a vulnerability is announced and when it is remediated by organizations.

Pre-emptive Security

Zero Day Attacks are the worst-case scenario for any business since they cannot be mitigated until after the damage is done.

Unfortunately, existing application security technologies provide little or no protection against this class of attack.

A well implemented RASP engine, however, provides pre-emptive security by disabling the vectors commonly exploited by Zero Day Attacks.

For example, a RASP-enabled Java Virtual Machine can be configured to deny the creation resources required to open network connections, and access databases or files.

The engine can deny the creation resources entirely if the application has no need of them, or it allows the creation for specific resources an application requires.

The escalation in the number and sophistication of application layer attacks has reached critical mass.

According to the most recent Verizon Data Breach Investigation Report, attacks on web applications were the single-biggest source of data loss.

As a result, we need an evolved approach to application security that provides self-protection in the run-time.

About the Author

John Matthew Holt is founder and Chief Technology Officer of Waratek. He is a recognized expert in Java, virtualization and application security, and chief architect of Waratek s application security platform.

John Matthew has been awarded more than 50 patents for inventions that span abstract machine, dynamic recompilation, distributed computing and virtualization technologies.

SOPHISTICATION OF CYBER ATTACKS CREATES ERA OF INTERNET SECURITY AS A RIGHT



LUIS CORRONS

Technical Director,
PandaLabs

There are a mix of exciting and frightening feelings when one takes a look into the future. Nowadays we rely on computers for everything. From household appliances to our cars, all of them are using software. It s not just consumer uses either, our utility companies that provide basic services such as running water or electricity could not run without software.

People say that Internet has changed our life, while true, it doesn t tell the whole story. What has really changed our lives is software. And it is a good thing, as it makes our lives easier and more comfortable. We are incorporating it into everything, from thermostats to lightbulbs, and the innovations in hardware and software allow really useful applications. We are all excited with the different autonomous car projects, I am pretty sure our grandchildren will think we are freaks because we had to drive vehicles by ourselves. What a bunch of primitive elderly guys And some of you even enjoyed that

The computer security industry is young, yet it has evolved dramatically ever since its inception less than 30 years ago. From fighting against viruses trying to infect files in a computer, spreading from one to another through floppy disks to professional criminal gangs running ransomware schemes and nation state sponsored attacks trying to influence other countries election processes or sabotaging nuclear programs.

In the beginning computer security was almost anecdotal, people were not concerned as it had no effect in their lives. The fact is that the more our lives depend on software, the more that concern grows. Today we store all kind of data digitally (from music or photos to our financial information) and we want to keep it safe. But security is not just about keeping our information safe, it is about having access to all services that makes our life more comfortable. Some might remember the film The Net, from 1995. The plot was about a young computer programmer - Sandra Bullock- who discovered a conspiracy and the bad guys tried to get rid of her hacking into all her information, hacking into the FBI databases to change her identity and make here pass as a criminal, etc. Back then, most people considered it science fiction. Not anymore, and those who watch the TV show Mr. Robot know what we are talking about here.

And here it is where the frightening feelings surface. If we try to translate the threats we are currently facing into our near future lives, it is scary. Going back to the autonomous cars, it is easy to picture an equivalent to the ransomware attacks abducting our car: either you pay or you cannot access your car. But that is just the tip of the iceberg: what do we value more than anything Our lives and the lives of the ones we love and care about. We have already seen remote attacks taking full control of cars that are in the road… who wouldn t give all their money to save her kids of a certain death

This is just an example that can be extrapolated to any other aspect in life where technology will be involved, which is basically EVERYTHING. It is time to wake up and realize that we cannot continue like this. It is time for strict security standards or all the excitement we have will turn into fear and chaos. We all have to be involved in this, and I am not just talking about the security industry. Governments, hardware and software makers have to be aligned to ensure that security is a priority.

About the Author

Luis Corrons has been working in the security industry for more than 17 years, specifically in the antivirus field. He is the Technical Director at PandaLabs, the malware research lab at Panda Security. Luis is a WildList reporter, member of the Board of Directors at AMTSO (Anti-Malware Testing Standards Organization) and member of the Board of Directors at MUTE (Malicious URLs Tracking and Exchange). He is also a top rated industry speaker at events like Virus Bulletin, HackInTheBox, APWG, Security BSides, etc. Luis also serves as liaison between Panda Security and law enforcement agencies, and has helped in a number of cyber-criminal investigations.

SEPARATING FACT FROM FICTION
THE TRUTH ABOUT THE DARK WEB



EMILY WILSON

Director of Analysis,
Terbium Labs



DR. CLARE GOLLNICK

Chief Data Scientist,
Terbium Labs

As a dark web data intelligence company we often get the question "What's actually on the dark web "

We're glad you asked.

In my conversations about the dark web, I often hear myths and rumors quoted as fact: red rooms, terrorist plotting forums, live auctions for human trafficking, chemical weapons. The reality of the dark web is quite a bit different.

About the Study:
Terbium Labs runs Matchlight, the first fully private, fully automated dark web data intelligence system. Matchlight is designed to alert customers the moment their information appears online where it shouldn't. To do that, and do it well, our system is backed by an unparalleled dark web search system that continuously crawls the unsavory parts of the internet in search of stolen data.

Most people never access the dark web. For those of us that do, there are few resources that allow for exploration or meticulous study. Even seemingly straightforward questions, like what kind and how much of different types of content exist on the dark web, do not have reliable answers.

Past industry reports have superficially addressed these questions but often include numbers and conclusions without explanations of where the data came from or how those numbers were computed.

We set out to do research in a way we hadn't seen it done in our space: using a random sample of Tor Hidden Service (.onion) URLs from a single day in our crawler's history, analyzing the results of that sample to get a representative measure of dark web content. We're a team of scientists at heart, and we value our methodology above all else (for detailed notes on methodology, see the full report here). By being transparent, we provide an opportunity for others to review and critique our data and to interpret our research with a level of scrutiny that would be expected of a scientific study.

Findings:
The results of our research may surprise you. It turns out the dark web is mostly legal, to the tune of almost 55% of the content sampled.

The dark web receives a fair amount of negative attention because of the anonymity it provides. To outside observers, the desire for anonymity goes hand-in-hand with criminal activity, and many summaries of the dark web focus exclusively on this criminal activity. As our data shows, however, most the dark web contains perfectly legal content.

What does legal content on the dark web look like These Tor Hidden Services play host to Facebook, European graphic design firms, Scandinavian political parties, personal blogs about security, and forums to discuss privacy, technology, even erectile dysfunction. Anonymity does not equate criminality, merely a desire for privacy.

Most discussions of the dark web entirely gloss over the existence of legal content. As the numbers above indicate, legal content comprises over half of all the domains sampled for our research, and nearly half of all pages we classified.

Came For The Drugs, Stayed For The Drugs:
What about the other half of our sample Of the illicit content in our sample, 45% was dedicated exclusively to the dark web drug trade.

The dark web drug trade, if we can call it that, is far more organized and mundane than you might expect. Purchases take place on moderated and well-maintained markets where buyers can drill down into categories and subcategories in search of the right vendor or product.

The drug community is a self-regulating, even a self-policing group. Vendors rely on reviews and commentary to build their brand and drive orders. New vendors are quick to offer free samples, and the community is more than happy to test a new product. Reviews follow a standard template, where users rank the stealth, shipping time, purity, high, and overall experience with the vendor and product.

The community quickly shuns known scammers as warnings pop up about disappearing packs or instances when buyers get less than what they paid for.

In addition to (recreational) drugs, our sample also revealed a steady trade in pharmaceuticals (11.9% of all illicit content). Dark web pharmacies provide unfettered access to prescription medications, recalled over-the-counter drugs, unapproved drugs, and unregulated supplements.

Take, for example, human growth hormones. Through the dark web, buyers in United States have access to a host of steroids that have not met FDA approval, or are pending approval in the United States.

Unlike recreational drugs, pharmaceutical vendors are more likely to invoke name brands or branded packaging in order to add legitimacy to their products, at least in part because pharmaceuticals are more difficult (if not impossible) for vendors to manufacture at home.

Carding: Yours, Not Mine, And Also Yours:
Dark web vendors have thoroughly systematized the fraud trade, offering everything from bank drops (bank accounts) to fullz (full identities) to payment cards or music-streaming credentials.

On certain dark web carding sites vendors sell batches of cards with few additional details; users simply purchase a certain number of cards from the vendor's stockpile and go on their way.

On other more sophisticated carding markets, users can sort and filter by bank, card type, city, state, issuer - a host of different options to narrow down a specific set of cards for purchase. Both vendors and buyers are facing falling validity rates on batches of cards as banks increasingly identify common points of purchase and shut down any active cards that may have been involved in a breach.

Why, then, does Fraud only make up 4.6% of our sample Many of the most prolific fraud sites technically exist on the clear web.

These clear web sites often operate on top level domains based in countries less likely to shut down sites hosting illegal activity: Western Samoa (.ws), Cameroon (.cm), Cocos Islands (.cc), and Oman (.om) are all favorite top level domains for fraud marketplaces.

The Persistent Myths and Unfortunate Truths:
Some myths about the dark web are just that - myths. Tales of interactive, live-streaming murders and dark web assassination services make headlines, but the reality is (for the most part) more mundane.

Other rumors, however, are unfortunately true. Child exploitation does exist on the dark web in a measurable quantity (for methodology on this category, see the full report here), as does extremism. Weapons sites do exist, though they are largely considered to be honeypots or scam sites.

Once More On Methods:
We always scrutinize data and methods (especially our own).

Terbium Labs has an academic mindset with strong roots in experimental science. We know that a single study is not definitive and that the scientific method is best applied with a healthy amount of scrutiny. Data never speaks for itself; data is not objective.

The following is a discussion of the limitations of our study, and others like it. We outline the assumptions we made in order to carry out this research. Taken together with the data itself, this allows for a more nuanced interpretation of our results.

A key conclusion of this study is that certain types of illicit activity, specifically weapons of mass destruction and extremism largely do not exist on the dark web. No amount of data can ever support a claim of absence .

This is not a limitation unique to our study, but a truth about the limits of inference. It is always possible that these sites are isolated from the rest of the dark web, or that our sample was not large enough to observe a specific example.

Even if we increased our sample size, the same logic still applies. This a problem that, unfortunately, plagues all data-driven endeavors. Our confidence intervals reflect this reality, providing acceptable ranges that should still be considered consistent with our results.

The Truth About the Dark Web

The dark web is host to primarily legal, even mundane content. The sections that aren't legal are dominated by drugs, fraud, and combinations of illegal activity - primarily the major dark web markets.

Just because the majority of the content is legal, though, doesn't mean it's safe. Legal content has the potential to be damaging, even dangerous. At Terbium, we refuse to make judgements about the kinds of information that would be interesting to our customers.

That's why we built out a big data infrastructure, backed by an unrivaled crawler. We want our customers to see everything that's on the dark web, not just the sites we think may be of interest.

There's always more research to be done. Within each of the categories we cover here, what types of content actually exist What percentage of the illegal content we captured is for sale, and what percentage is shared as free information What would these numbers look like if we expanded our sample beyond Tor Hidden Services

Research is hard, and data is not magic. At Terbium, we like hard questions.

About The Authors

Emily Wilson is the Director of Analysis at Terbium Labs. Emily is responsible for managing a team of analysts, while tracking industry news and trends among actors on the dark web, including specific breach operations, popular targets, and the appearance of new sites for trading or discussing stolen data. Emily provides analysis on the appearance of fraud, drugs, weapons, extremism, and other information appearing on the dark web.

Emily has a background in Eastern European politics, and holds a Bachelor of Arts in International Relations from The College of William & Mary. Emily can be reached online at (emily@terbiumlabs.com) and at our company website http://www.terbiumlabs.com/

Clare Gollnick is the Chief Data Scientist at Terbium Labs. As a statistician and engineer, she designs the algorithms that direct Terbium s automated crawl of the dark web and leads the crawler engineering team. Before turning her attention to the dark web, Clare was a neuroscientist. Her academic publications focus on information processing within neural networks and validation of statistical methods.

Clare holds a PhD in biomedical engineering from Georgia Tech and a B.S. in bioengineering from UC Berkeley. Clare can be reached online at (clare@terbiumlabs.com) and at our company website http://www.terbiumlabs.com/

DARK ENDPOINTS ARE A BREEDING GROUND FOR **SECURITY BREACHES**

You need always-on visibility and real-time remediation to stop security breaches at the source. And it's all possible with exclusive self-healing endpoint security from Absolute.

Absolute sees and secures what others cannot with the only solution that:

- Is embedded and impossible to remove from more than a billion popular devices
- Eliminates endpoint blind spots —on and off the network
- Remediates compromised endpoint controls instantly
- Reduces vulnerabilities to withstand user error or malicious attacks


IDC

IDC TECHNOLOGY SPOTLIGHT

Modern "Embedded" Endpoint Security: Gain Visibility into and Control of Data, Devices, and Applications Regardless of Location and Connectivity

November 2018

Sponsored by Absolute

Introduction

Learn more about how the self-healing endpoint from Absolute helps you protect devices, data, applications and users anytime, anywhere at **www.absolute.com/IDCreport**. Download the free report today.

/ABSOLUTE™

Always There. Already There.

ZONE VS. MAN:
WHICH SECURITY DEFENSE STRATEGY IS BEST?



KIM ELLERY

Director of Product Marketing, Absolute

Every year, we discuss the state of cybersecurity: *the sky is falling… we are no longer in control…* or *mobile this and cloud that…* Yes, these are all valid concerns that constantly shift the goalposts and inform the game plan of our industry. But as IT security professionals, we collectively need to step back and be reminded of our objective: enable business while protecting what matters most. And if this is the subjective definition of winning the game, it appears we are behind on the scoreboard.

If the news headlines are any indication, our defense has major holes and our offense is either non-existent, or at best, ineffective. The protection gap is getting wider by the day, with the opposition changing the rules with evolving tactics and increased evasion, and the deficit in skill resulting in a shortage of players to field a full defense unit.

Like a good team coach, it s time to huddle the players and take the game back to the fundamentals. This starts by assessing the opposition; evaluating the structure of our defense; and ensuring that if one tackle is missed, another teammate is always there to provide cover. If we can t see the opposition s plays, or even know where our own players are, there is no way we are going to be able to defend our game.

> *"Many will argue visibility is provided by existing tools, but legacy, perimeter-based approaches to security are ineffective for today's digital enterprise"*

Let s relate this analogy back to security: to be effective, we need visibility. Many will argue visibility is provided by existing tools, but legacy, perimeter-based approaches to security are ineffective for today s digital enterprise. If you can only see what is happening on your network, or are only defending against known external threats, the mobile this, cloud that sledgehammers will fracture any visibility you think you have. Accelerating technology adoption and business expectations is adding more fuel to the fire. According to Gartner "By 2021, 27% of corporate data traffic will bypass perimeter security (which is an increase from 10% from today) and flow directly from mobile and portable devices to the cloud.

> *"According to Gartner "By 2021, 27% of corporate data traffic will bypass perimeter security (which is an increase from 10% from today) and flow directly from mobile and portable devices to the cloud"*

If our visibility is fractured and blind spots continue to exist - with the devices outside our perimeter most at risk - we are unable to take effective preventative action. This is demonstrated by the average time to identify (MTTI) data breaches, which sits at a staggering 201 days. Gaining comprehensive visibility will reduce the time it takes to identify, and most importantly, to respond to a security incident, which better protects data and reduces operational expenses.

At its core, we can t secure what we can t see. If we can only see 90 percent of our devices, what s protecting the remaining 10 percent What are the chances that the one device you can t see is going to be the one that ends up in the wrong hands Poor visibility limits your team s ability to manually defend against threats, and security professionals are only just beginning to understand the enormity of the fragmentation issue.

Whether the cloud service or device is sanctioned or not, you need visibility into what applications are running, what data is being stored/shared in them, and who is using that data from which locations and devices. Fractured visibility is not good enough.

The historical model of your devices, your applications on your network has fallen apart, creating giant cracks. It s these cracks that attackers are exploiting. They just need to find an opening once and they are in, and chances are, they already have. Hackers know that overwhelmed security teams cannot defend against what they cannot see with this avalanche of activity.

We must prevent lack of visibility from being added to the repetitive chorus of other disruptive trends by:

Forgetting the concept of the perimeter. Security needs to go to where the user is, and that s everywhere.

- Focusing on the data you need to protect, going back to the key objectives.
- Looking at the agility of your application layer, specifically an application s ability to fend for itself if attempts are made to compromise it.
- Enabling critical security applications to provide the same level of visibility and control regardless of whether it s a desktop on your network or an employee s new tablet on the other side of the globe.
- Helping applications account for something we see every day in IT: questionable user behavior. Employees will disable, delete, and bypass security applications, either maliciously or negligently.
- Strengthening investments with self-hardening technologies that adapt for these scenarios. This will expand your horizons from only seeing what is healthy and under control, to all of the devices, data, and applications you need to secure.

To gain a complete picture of vulnerabilities, organizations need endpoint and application monitoring technologies to reduce the attack surface, and when necessary respond accurately and quickly to attacks in progress. Understanding baselines, normal behavior and risk thresholds will allow you to quickly identify variations and emerging threats and respond appropriately.

As the traditional perimeter-based model becomes less effective, the focus must shift to the endpoints, as these are the opening to your organization and a typical target for intrusion.

Strengthening our defenses in key positions encourages the entire team to work harder, become more resilient and hopefully react better. In cybersecurity, if you balance your emphasis on not only detecting threats, but also predicting the plays before they take place, you ve made the first step toward putting an all-star defensive team on the field.

Just like making sure you ve got a quarterback who has great peripheral vision and can see threats coming, if you make visibility a core priority, you ll be better equipped to see what you really need to protect and put the appropriate security controls in place.

Threats don t occur in a vacuum, so expect the unexpected... when you see the blitz coming, you ll have the tools in place to stop the sack.

About the Author

Kim Ellery is Director of Product Marketing at Absolute, where he leads the development and execution of the company s go-to-market strategy. He also works with the Absolute executive team to define an overall product and technology strategy that enables the long-term growth and strategic direction of the company.

95% OF BREACHES HAPPEN BEHIND FIREWALLS ON SYSTEMS PROTECTED BY THE LATEST ANTI-VIRUS

Only one company stops these breaches

www.snoopwall.com

WITH OUR PATENTED, AGENTLESS COST EFFECTIVE, PLUG-AND-PLAY NETSHIELD APPLIANCES

NANO
25 & 100



Branch PRO

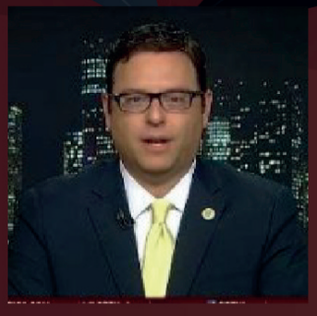


Enterprise 10/100/250/1000



Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

7 SECRETS OF OFFENSIVE SECURITY



GARY MILIEFSKY

The State of Network Security Today – Reactive and Slow

Network breaches are in the news every day. In the US alone, there have been over 900,000,000 – that s 900M records of personally identifiable information (PII) stolen over the past few years. While most organizations are running the latest corporate firewalls – also known as UTMs – unified threat management systems or NGs – next generation firewalls and the latest and greatest antivirus products, they are still breached. Over 95% of breaches happen behind these corporate firewalls on these endpoints that appear allegedly to be secured by antivirus.

So, it seems, the hackers have leap-frogged most INFOSEC countermeasures. Yes, that s what the tools you ve been buying to protect yourself are – just reactive technologies, countermeasures, that usually react too late – causing a ransomware payment decision, data theft, downtime or even much worse.

The Way to Win the Battle – Proactive, Offensive, Fast and Semi-Automated

While not all of your defenses can be automated, I do like to focus on more proactive approaches to the problem of being breached. If you do a root-cause analysis, you will discover your weaknesses in advance of their exploitation. For example, let s say you buy the latest and greatest antivirus software, keep it always up to date and then get infected. The infection exploits a fairly new but known vulnerability in the Microsoft Windows RPC protocol, which can be found in the nvd.nist.gov database on common vulnerabilities and exposures (CVEs). While your antivirus software focuses on reacting – scrubbing and cleaning up after you ve been infected, it s still reactive technology. The Offensive security model suggests you should find out which systems have the RPC vulnerability, contact Microsoft for a patch and fix this hole quickly. If there is no patch available, maybe you could turn off the RPC protocol for a few days or a week until next week s Patch Tuesday from Microsoft. Better to lock your network down from the inside-out, where breaches happen because of internal weaknesses – people and computers are extremely vulnerable.

Let s explore the 7 secrets of Offensive Security and learn a new, more proactive approach to dealing with protection of PII, keeping networks running and employees productive. We ll dig into ideas and methods that, while they sound so simple and easy, sometimes to implement them, you ll be dealing with corporate politics, budget issues, resource issues and time constraints.

I ll go into a deep dive for you on each of these seven secrets, however, let s get started right away, here are my seven secrets:

- Demand Executive Support – Funding, Training, Etc.
- Deploy Continuous (Or Daily At Minimum) Backups And Test Them – Does The Restore Even Work
- Deploy Corporate Wide Encryption
- Create A living Corporate Security Document
- Train (And Retrain) All Employees On Best Practices Infosec Policies(ISO27001, COBIT, NIST– Choose One You Like)
- Manage The Bring Your Own Devices (BYOD) Dilemma By Assuming All Mobile Devices Already Infected
- Deploy And Manage A Breach Prevention Solution (We ll Quickly Show You Ours) That Helps…

  a) Document and mitigate RISK, especially serious vulnerabilities (CVEs)
  b) Provide Network Access Control (NAC)
  c) Quarantine high-risk, rogue and infected devices

What is the real cost of a Breach?
Recently, the Ponemon Institute concluded it s 2016 Data Breach report. According to this report (excerpted under fair use of the US Copyright Act, source: http://www.ibm.com/security/data-breach):

The cost of data breach sets new record high. According to this year s benchmark findings, data breaches cost companies an average of $221 per compromised record – of which $145 pertains to indirect costs, which include abnormal turnover or churn of customers and $76 represents the direct costs incurred to resolve the data breach, such as investments in technologies or legal fees.

The total average organizational cost of data breach reaches a new high. In the past 11 years, the most costly organizational breach occurred in 2011, when companies spent an average $7.24 million. In 2013, companies experienced a net decrease in total data breach cost to $5.40 million. This year, the total average cost is $7.01 million.

Measures reveal why the cost of data breach increased. The average total cost of a data breach grew by 7 percent and the average per capita cost rose by 2 percent. Abnormal churn of existing customers increased by 3 percent. In the context of this paper, abnormal churn is defined as a greater than expected loss of customers in the normal course of business. The average size of a data breach (number of records lost or stolen) increased by 5 percent. Certain industries have higher data breach costs. Heavily regulated industries such as healthcare, life science and financial services, tend to have a per capita data breach cost substantially above the overall mean of $221. In contrast, public sector (government), hospitality and research had a per capita cost well below the overall mean value.

Malicious or criminal attacks continued to be the primary cause of data breach. Fifty percent of incidents involved a malicious or criminal attack, 23 percent of incidents were caused by negligent employees, and 27 percent involved system glitches that included both IT and business process failures.

Malicious attacks were most costly. Companies that had a data breach due to malicious or criminal attacks had a per capita data breach cost of $236, significantly above the mean of $221. In contrast, system glitches or human error as the root cause had per capita costs below the mean ($213 and $197, respectively).

Certain industries were more vulnerable to churn. Financial, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research organizations tend to experience a relatively low abnormal churn.

The more records lost, the higher the cost of data breach. This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

The more churn, the higher the per capita cost of data breach. Companies that experienced less than 1 percent churn, or loss of existing customers, had an average organizational cost of data breach of $5.4 million and those experiencing churn greater than 4 percent had an average cost of data breach of $12.1 million.

Certain industries were more vulnerable to churn. Financial, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research organizations tend to experience a relatively low abnormal churn.

Detection and escalation costs are at a record high. These costs include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. Average detection and escalation costs

increased dramatically from $0.61 million to $0.73 million, suggesting that companies are investing more heavily in these activities.

Notification costs increased slightly. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary mail contacts or email bounce-backs and inbound communication set-up. This year s average notification costs increased slightly from $0.56 million in 2015 to $0.59 million in the present year.

Post data breach costs increased. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. These costs increased from $1.64 million in 2015 to $1.72 million in this year s study.

Lost business costs increased. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The current year s cost of $3.97 million represents an increase from $3.72 million in 2015. The highest level of lost business cost was $4.59 million in 2009.

Companies continue to spend more on indirect costs than direct costs. Indirect costs include the time employees spend on data breach notification efforts or investigations of the incident. Direct costs refer to what companies spend to minimize the consequences of a data breach and to assist victims.

These costs include engaging forensic experts to help investigate the data breach, hiring a law firm and offering victims identity protection services. This year the indirect costs were $145 and direct costs were $76.

The bottom line is this: Breaches are EXTREMELY costly and may put your organization out of business and you, out of a job.

Isn t it time to take an Offensive approach to cyber security Aren t you tired of reading about breaches in the news, wondering if your organization will be next

Are Insider Threats Really That Serious?

The proof is in the pudding – according to PrivacyRights.org we ve seen nearly ONE BILLION PII RECORDS stolen in the USA alone (see http://www.privacyrights.org and click on chronology of data breaches) not including the Yahoo breach. You ll see most of these breaches are starting to happen on Small to Medium Sized Enterprises (SMEs) more than ever before.

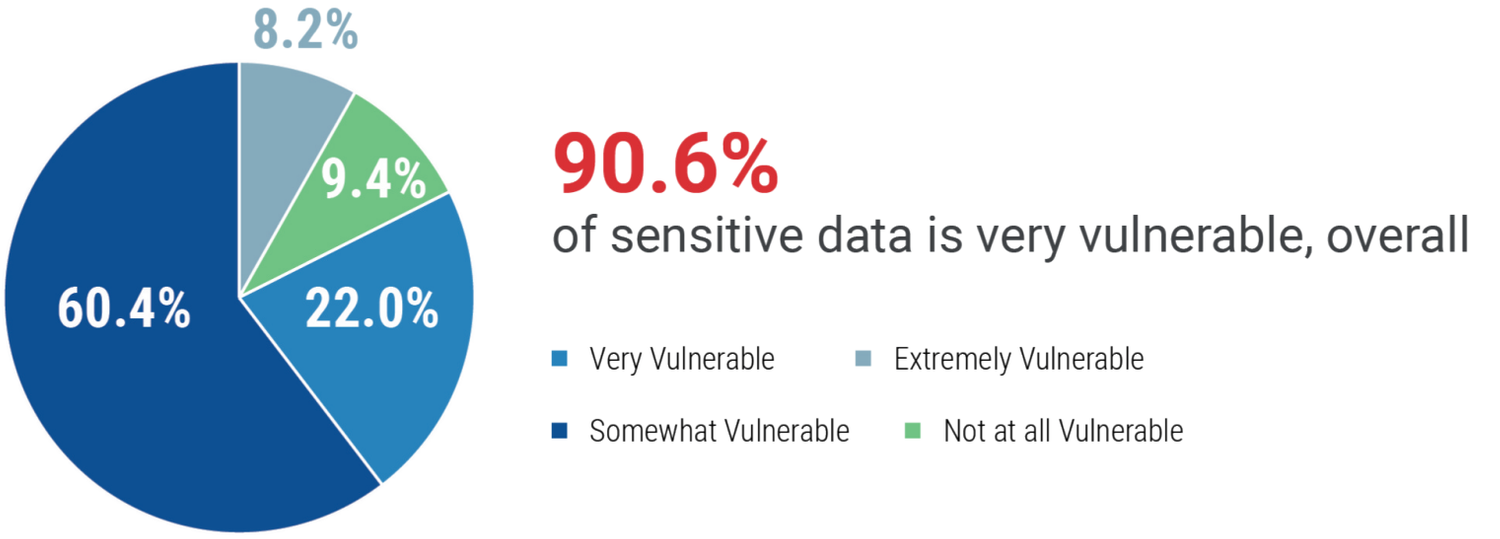
SMEs have become the #1 target of cyber breaches because they are easier targets than those like a Bank of America who has a $400M per year Cyber Security budget and a huge INFOSEC team protecting their networks 7x24x365 and who can weather a major breach, as they manage over $4 TRILLION US DOLLARS.

The only way to get ahead of a breach is to not let it happen and if it does, to instantly, quickly, automatically isolate it and minimize the impact.

So, now that you ve seen how costly breaches are and you ve also now know my 7 secrets of Offensive Security, let s discuss each one in more detail.

Demand Executive Support

This may not be easy, however, you will have to get the Board of Directors, the CEO, CFO, CIO, etc., all top level executives to agree that, fiduciarily, the right thing to do to avoid a breach is to have an annual budget, agree that training of all employees is important, that a corporate security policy is a must have and how the corporation will react if and when a breach actually does happen.



Deploy Continuous Backups and Test Them Regularly

When is the last time you tested a restore of a backup file When did you most recently backup employee desktops, laptops, servers and other critical infrastructure While there are numerous and very solid backup pr smaller list of continuous data protection products that are doing backups in real-time.

Continuous data protection (CDP),also called continuous backup or real-time backup, refers to backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves.

Deploy Corporate-wide Encryption

Encryption is one of the most powerful ways to protect personally identifiable information (PII). There s encryption for data in transit, encryption for entire hard drives, databases and file systems. If you have employees who travel frequently, if there were a way to encrypt their smartphone, tablet, laptop, netbook and notebook hard drives and file systems that would be the best place to encrypt first – in many cases employee traveling equipment are lost or stolen and without encryption, whatever corporate records, data, passwords, VPN client or other confidential information could end up in the hands of criminals or other preying eyes. If there s ever a breach either on portable equipment or behind the corporate firewall, you can mitigate data theft risk, if the data that s accessible to the hackers and cyber criminals is encrypted and they don t have the keys.

Create a "Living" Corporate Security Document

A living corporate security policy is your documentation that states in writing how your organization plans to protect the company's physical and information technology (IT) assets. It s a living document because it s never final. Most corporate security policies include acceptable use, password management, network access control, bring your own device policies, encryption policies and others with descriptions on mitigating risk and how policies are to be enforced. You ll also want to deploy policies that help you prove due care and due diligence in compliance with regulations that affect your organization (FISMA, EU GDPR, GLBA, SOX, HIPAA-HITECH, VISA PCI, etc.).

Train and Retrain All Employees on Best Practices INFOSEC Policies

So, now you have a great living corporate security policy. Do your fellow employees from the C levels down to the receptionist understand these policies Are they helping you implement them or are they becoming difficult and a hindrance to your documented regulatory compliance and best practices Of all the policies you re implementing,

which one s will most likely cause a breach or data theft, if an employee violates the policy

The most important would be a Bring Your Own Device policy (BYOD) as it s a network asset that you are allowing to cross the bounds, outside of your firewall and then returning, most likely in a different (maybe infected, maybe more insecure) state. Others include ensure devices have the latest patch and application updates, as well as proper configuration and system hardening, to reduce the risk of Common Vulnerabilities and Exposures (CVEs) that get exploited by hackers, cyber criminals and malware.

Antivirus software should be up to date but it won t stop the latest exploits – especially Spear Phishing, Remote Access Trojans (RATs) and Ransomware. This requires a better educated employee population who understand that sending and receiving un-encrypted emails is a big risk, emails with attachments and being too trusting to click links and open attachments without verifying the senders true identities. This leaves them wide open to being socially engineered and victimizing your organization.

Manage the Bring Your Own Devices (BYOD) Dilemma

Bring your own device (BYOD) has become pervasive. Most companies are being pressured by their executives for cost reduction and productivity boosting, to allow employees to bring their personally owned devices (laptops, tablets and smartphones) to work. They are asking for privileges to, either behind the firewall over corporate wifi, or over the public internet using 3G/4G or public wifi, to be able to VPN into corporate resources from these traveling devices. There could not be a riskier thing to do, when it comes to corporate security. Mobile freeware is usually spyware – from Flashlight apps to Emoji Keyboards and QR readers…they are spying on you and sending data to other countries.

Deploy and Manage a Breach Prevention Solution

You have a firewall. Check. You have anti-virus. Check. Ok, so now you are about 5% protected. Now is the time to deploy a breach prevention solution because over 95% of breaches happen behind the corporate firewall on systems running the latest antivirus software. Can you tell if a system has a critical vulnerability that is easily exploitable Do you know if the Cleaning Company is plugging in a rogue device on your network this evening What about an employee who forgot about your spear-phishing policy and just clicked a link leading to an installation of Locky Ransomware that will probe your corporate network to attempt to encrypt not only the employee desktop but all of your fileservers How do you get one step ahead of these threats With a breach prevention solution.

About the Author

Gary is the CEO of SnoopWall, Inc. and a co-inventor of the company s innovative breach prevention technologies. He is a cyber-security expert and a frequent invited guest on national and international media commenting on mobile privacy, cyber security, cyber-crime and cyber terrorism, also covered in both Forbes and Fortune Magazines. He has been extremely active in the INFOSEC arena, most recently as the Editor of Cyber Defense Magazine.

Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), the National Information Security Group (http://www.NAISG.org) and the OVAL advisory board of MITRE responsible for the CVE Program (http://CVE.mitre.org). He also assisted the National Infrastructure Advisory Council (NIAC), which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace as well as the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Previously, Gary has been founder and/or inventor for technologies and corporations sold and licensed to Hexis Cyber, Intel/McAfee, IBM, Computer Associates and BlackBox Corporation. Gary is a member of ISC2.org and is a CISSP®.

CYBERSECURITY PAVILION

NABSHOW
Where Content Comes to Life

NAB Show is proud to announce the NEW Cybersecurity Pavilion debuting April 22-27, 2017 at the annual event in Las Vegas.



In a 2016 survey of over 103,000 broadcast industry attendees, over **40%** were worried about breaches, ransomware and denial of service & want cybersecurity on the agenda.

This is a great opportunity to help educate and protect the Broadcast Media market from Cybercrime, Cyberterrorism, and DDoS attacks.

CONTACT US TODAY: **Grant Samples** gsamples@nab.org 202-429-4184



KEYNOTE SPEAKER: Gary S. Miliefsky

Globally Recognized Breach Prevention Expert
"Offensive Cybersecurity for Broadcast Media"

PLATINUM MEDIA SPONSOR: CDM

KEYNOTE SPONSOR: SnoopWall

PLATINUM INFOSEC SPONSOR: DELL EMC

2017 PREDICTIONS



PIERLUIGI PAGANINI

Editor-in-Chief,
CDM

As in years past, let s try to anticipate the coming cybersecurity trends, starting from events observed in the last 12 months. Which are the predictions for 2017 in terms of threats and cyber criminal phenomena

Once again malware, ransomware first of all

The threat landscape will be characterized by a significant increase of malware, especially ransomware and malicious code designed to infect mobile devices. Ransomware has become one of the fastest growing threats, the trend will continue in the next year and the criminal underground will develop new malicious code with sophisticated features. The improvement will be focused on features that allows ransomware to avoid detection and rapidly spread among the greatest number of machines. The number of new Ransomware families is expected to increase such as the number of ransom-as-a-service platforms.

Nation state hacking is the main topic of a global cyber agenda

Nation state hacking will be one of the main cyber threats for states worldwide. The alleged interference of Russian Government in 2016 interference is just the tip of the iceberg of an intense activity conducted by almost any nation-state actor. Information Warfare is one of the most important topics for the cyber strategy of any states and global association of governments. The number of campaigns conducted by state-sponsored hackers will increase and states urge norms of state behaviors in order to control the proliferation of cyber weapons.

IoT devices, a dangerous weapon in the wrong hands

The number of internet of Things device will continue to increase such as the level of penetration of smart objects in almost any industry. The number of cyber attacks against IoT devices will increase due to the lax of security by design and poor security settings. The situation is serious, IoT vendors will continue to design devices that in many cases totally ignores cyber security fundaments. It is easy to predict the development of new families of IoT malware and criminal services that leverage on botnet of compromised smart objects (i.e. DVRs, Routers, CCTVs). The pervasiveness of smart devices across various industries will enable further DDoS attacks through thingbots infected by IoT malware like Mirai. IT industry urges of a regulatory response for the manufacturing of a new generation of secure devices.

Cybercriminals focus on crypto currencies

Many experts speculate that crypto currencies could assume an important role in the global economy, some currencies like the Bitcoin will represent a valid asset on which invest when the value of local currency is dropping. This means that the high demand of cryptocurrency will make their value to increase attracting the cyber crime. Cyber criminals will continue to detect malware specifically designed to steal crypto currencies or to abuse victim s resources for mining activities. The Zcash currency will probably offer the greatest financial opportunity to criminal syndicates, it will be one of the most profitable currencies along with Bitcoin.

The year of the Artificial Intelligence

Is the Artificial Intelligence a panacea for the IT security industry A growing number of companies will start implementing AI-based solutions, especially for the protection of critical infrastructure. AI could be used to detect zero-day attacks, new technologies will allow to reduce the time of detecting new threats.

The number of cyber attacks will continue to grow almost in every industry.

It is too easy to predict a constant increase of cyber attacks in the wild. Healthcare, energy, and retail will be the sectors most targeted by cyber criminals. SMBs will continue to be the most exposed to this wave of cyber attacks. The attacks against SCADA (*supervisory control and data acquisition)* and Industrial control systems (ICS) will be among top cyber threats in 2017. Industrial control systems (ICS) continue to be a privileged target of hackers. We will observe an increase in the brute force attacks on supervisory control and data acquisition (SCADA) systems.

CDM INFOSEC AWARDS 2017



waratek

Waratek Runtime Application Self Protection (RASP)

"The Leader in Application Security Solutions for 2017" - CDM



acunetix

Acunetix Vulnerability Scanner

"The Cutting Edge Web Application Solution for 2017" - CDM



RISKSENSE™
TRANSFORMING CYBER RISK MANAGEMENT

RiskSense Platform

"The Editor's Choice in Risk Management Solutions for 2017" - CDM



jumio®

Jumio Netverify™

"The Cutting Edge Biometrics Solution for 2017" - CDM



bitglass
total data protection

Bitglass CASB Solution

"The Hot Company in Cloud Security Solutions for 2017" - CDM



RISKSENSE™
TRANSFORMING CYBER RISK MANAGEMENT

RiskSense Platform

"The Leader in Vulnerability Management Solutions for 2017" - CDM



ANOMALI

Anomali ThreatStream

"The Next Gen Threat Intelligence Solution for 2017" - CDM



Dtex User Threat Platform

"The Leader in Insider Threat Detection Solutions for 2017" - CDM



RiskVision Platform

"The Hot Company for Risk Management Solutions for 2017" - CDM



Indegy

Indegy Industrial Cyber Security Platform

"The Next Gen ICS/SCADA Security Solution for 2017" - CDM



ENDGAME.

Endgame Endpoint Security

"The Most Innovative Endpoint Security Solution for 2017" - CDM



HERJAVEC GROUP

Herjavec Group

"The Best Identity & Access Management Solution for 2017" - CDM



HEXADITE

Hexadite Automated Incident Response Solution

"The Leader in Incident Response Solutions for 2017" - CDM



GURUCUL
PREDICTIVE SECURITY ANALYTICS

Gurucul Risk Analytics (GRA)

"The Best User Behavior Analytics Solution for 2017" - CDM



Attivo NETWORKS®

Attivo BOTsink

"The Next Gen Deception Based Security Solution for 2017" - CDM



illumio

Illumio Adaptive Security Platform™(ASP)

"The Best Data Center Security Solution for 2017" - CDM



CLAROTY
Clarity for OT Networks

Claroty Platform

"The Leader in ICS/SCADA Security Solutions for 2017" - CDM



Bay Dynamics®

Bay Dynamics Risk Fabric

"The Most Innovative Risk Management Solution for 2017" - CDM



FireEye®

FireEye Network Security

"The Leader in Network Security Solutions for 2017" - CDM



whiteCryption®
an Intertrust Company

whiteCryption Cryptanium

"The Hot Company in Application Security Solutions for 2017" - CDM



illumio

Illumio Adaptive Security Platform™(ASP)

"The Best Cloud Security Solution for 2017" - CDM



SIEMPLIFY

Siemplify ThreatNexus

"The Cutting Edge Incident Response Solution for 2017" - CDM



CyberX

CyberX Automated ICS Vulnerability Assessment

"The Hot Company in Vulnerability Management Solutions for 2017" - CDM



BUFFERZONE

BUFFERZONE Endpoint Security Solution

"The Leader in Endpoint Security Solutions for 2017" - CDM



CITRIX®

Citrix NetScaler AppFirewall

"The Cutting Edge Application Security Solution for 2017" - CDM



Dome9 SECURITY

Dome9 Arc SaaS Platform

"The Editor's Choice in Cloud Security Solutions for 2017" - CDM



DARKTRACE

Darktrace Enterprise Immune System

"The Best Enterprise Security Solution for 2017" - CDM



savvius™

Savvius Omnipeek

"The Most Innovative Forensics Solution for 2017" - CDM



TRAPX SECURITY

TrapX DeceptionGrid

"The Hot Company for Deception Based Security Solutions for 2017" - CDM



observe it

ObserveIT Endpoint Solution

"The Most Innovative Insider Threat Prevention Solution for 2017" - CDM



HERJAVEC GROUP

Herjavec Group Managed Security Services

"The Hot Company in Managed Security Service Providers (MSSP) for 2017" - CDM



Cyber adAPT

Cyber adAPT Platform

"The Editor's Choice in Mobile Endpoint Security Solutions for 2017" - CDM



KGSS
CYBERSECURITY FOR A SAFER WORLD

KGSS Intelligence Reports

"The Best Threat Intelligence Solution for 2017" - CDM



portnox™
boundlessly smart

Portnox CLEAR™

"The Cutting Edge Cloud Security Solution for 2017" - CDM



Centrify®

Centrify Identity Service

"The Most Innovative Identity & Access Management Solution for 2017" - CDM



CyberX Automated ICS Vulnerability Assessment

"The Best ICS/SCADA Security Solution for 2017" - CDM



DefenseStorm Platform

"The Cutting Edge Risk Management Solution for 2017" - CDM



cybereason

Cybereason Platform

"The Hot Company for Incident Response Solutions for 2017" - CDM



ThreatTrack

ThreatTrackThreatSecure®

"The Best Anti-Malware Solution for 2017" - CDM



aqua

Aqua Container Security Platform

"The Most Innovative Application Security Solution for 2017" - CDM



netskope

Netskope Active Platform

"The Leader in Cloud Security Solutions for 2017" - CDM



NYOTRON
SECURING THE WORLD

Nyotron Paranoid

"The Hot Company for Endpoint Security Solutions for 2017" - CDM



NOZOMI
NETWORKS

Nozomi Networks SCADAguardian

"The Cutting Edge ICS/SCADA Security Solution for 2017" - CDM



SECDO

SECDO IR Platform

"The Editor's Choice for Incident Response Solutions for 2017" - CDM



corero
FIRST LINE OF DEFENSE

Corero SmartWall Threat Defense System

"The Best Network Security Solution for 2017" - CDM



CISCO

Cisco Stealthwatch

"The Leader in User Behavior Analytics Solutions for 2017" - CDM



TERBIUM LABS

Data Intelligence

Terbium Labs Matchlight

"The Most Innovative Threat Intelligence Solution for 2017" - CDM



cybereason

Cybereason Platform

"The Cutting Edge Endpoint Security Solution for 2017" - CDM



CYBRIC

Cybric SaaS Platform

"The Editor's Choice in Enterprise Security Solutions for 2017" - CDM



CloudPassage

CloudPassage Halo

"The Most Innovative Cloud Security Solution for 2017" - CDM



EdgeWave™

EdgeWave ePrism Email Security

"The Best Messaging Security Solution for 2017" - CDM



Skycure

Skycure Platform

"The Next Gen Mobile Endpoint Security Solution for 2017" - CDM



AppSense®

AppSense Application Manager

"The Most Innovative Data Center Security Solution for 2017" - CDM



GuardiCore

GuardiCore Centra Security Platform

"The Leader in Deception Based Security Solutions for 2017" - CDM



RISKIQ

RiskIQ Enterprise Digital Footprint

"The Best Digital Footprint Security Solution for 2017" - CDM



deepinstinct

Deep Instinct Platform

"The Hot Company in Anti-Malware Solutions for 2017" - CDM



ABSOLUTE®

Absolute Application Persistence

"The Editor's Choice in Application Security Solutions for 2017" - CDM



blacksands

blacksands' Secure Connection as a Service

"The Best Access Control Solution for 2017" - CDM



LogRhythm™

The Security Intelligence Company

LogRhythm Security Intelligence & Analytics Platform

"The Hot Company in Security Information Event Management Solutions (SIEM) for 2017" - CDM



NU Data Security

NuData NuDetect

"The Best Biometrics Solution for 2017" - CDM



fireglass

Fireglass Threat Isolation Platform

"The Cutting Edge Network Security Solution for 2017" - CDM



empow
You have it in you.

empow Platform

"The Editor's Choice in Security Abstraction Solutions for 2017" - CDM



LogRhythm™
The Security Intelligence Company

LogRhythm Network Monitor (NetMon)

"The Best Forensics Solution for 2017" - CDM



Haystax TECHNOLOGY

Haystax Constellation Analytics Platform™

"The Editor's Choice in Insider Threat Prevention Solutions for 2017" - CDM



plainID
AUTHORIZATION MADE SIMPLE

PlainID Platform

"The Next Gen Identity & Access Management Solution for 2017" - CDM



EdgeWave™

EdgeWave iPrism Web Security

"The Best Content Management & Filtering Solution for 2017" - CDM



exabeam

Exabeam's User Behavior Analytics (UBA)

"The Editor's Choice in User Behavior Analytics Solutions for 2017" - CDM



APERIO

APERIO Systems Platform

"The Hot Company in ICS/SCADA Security Solutions for 2017" - CDM



untangle™

Untangle NG Firewall

"The Editor's Choice in Firewall & VPN Appliances for 2017" - CDM



ZIMPERIUM

Zimperium Mobile Threat Protection

"The Next Gen Bring Your Own Device (BYOD) Solution for 2017" - CDM



BlueTalon

BlueTalon Data-Centric Security Platform

"The Editor's Choice in Data Centric Security Solutions for 2017" - CDM



acunetix

Acunetix Vulnerability Scanner

"The Best Vulnerability Management Solution for 2017" - CDM



SPIRION

Spirion Platform

"The Editor's Choice in Data Leakage Prevention (DLP) Solutions for 2017" - CDM



DEMISTO

Demisto Enterprise

"The Best Incident Response Solution for 2017" - CDM



CRONUS
CYBER TECHNOLOGIES

Cronus CyBot MSSP

"The Most Innovative Managed Security Service Provider (MSSP) for 2017" - CDM



TREASURE DATA

Treasure Data Live Data Management Platform

"The Best Software as a Service(SaaS) Solution for 2017" - CDM



CYLANCE

CylancePROTECT®

"The Most Innovative Anti-Malware Solution for 2017" - CDM



OASIS TECHNOLOGY

Oasis Technology Titan

"The Best Intrusion Prevention Solution for 2017" - CDM



wombat™ security technologies

Wombat Security Training

"The Leader in Security Training for 2017" - CDM

SIGN UP FOR CYBER WARNINGS MONTHLY E-MAGAZINE

www.cyberdefensemagazine.com







Cyber Defense Magazine, CDM and Cyber Warnings are Trademarks of STEVEN G. SAMUELS LLC. All rights reserved worldwide. Copyright © 2017, Cyber Defense Magazine. Portions may be copyright by our writers. Contact us for reprint rights.

All rights reserved. No part of this magazine may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Contact us for redistribution rights.

Because of the dynamic nature of the Internet, any Web addresses or links contained in this magazine may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

Cyber Defense Magazine
EIN: 454-18-8465, DUNS# 078358935.

All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

Cyber Defense Magazine

The Experts Agree.

Secure Enterprise-ready File Transfer Software • Works on multiple platforms • GoAnywhere.com



Download the Report And See For Yourself

Learn how GoAnywhere stacks up against the competition in this independent study from Info-Tech Research Group. The in-depth report includes strategies for researching an MFT solution along with a comparison of current MFT products from various vendors.

GO ANYWHERE™
Managed File Transfer

INSTANTLY Download the complete report for FREE and watch the accompanying 5 minute video on Selecting and Implementing a Managed File Transfer Solution by visiting:

GoAnywhere.com/infotech

800-949-4696

LINOMA SOFTWARE

Visit us at RSA! North Expo: Booth 4407

- Simplify, Encrypt and Automate File Transfers
- Enterprise-ready & Scalable
- Detailed Reporting for Compliance
- Multi-platform, Affordable & User-friendly

VENDOR LANDSCAPE AWARD — LEADER — Info-Tech

VENDOR LANDSCAPE AWARD — BEST OVERALL VALUE — Info-Tech