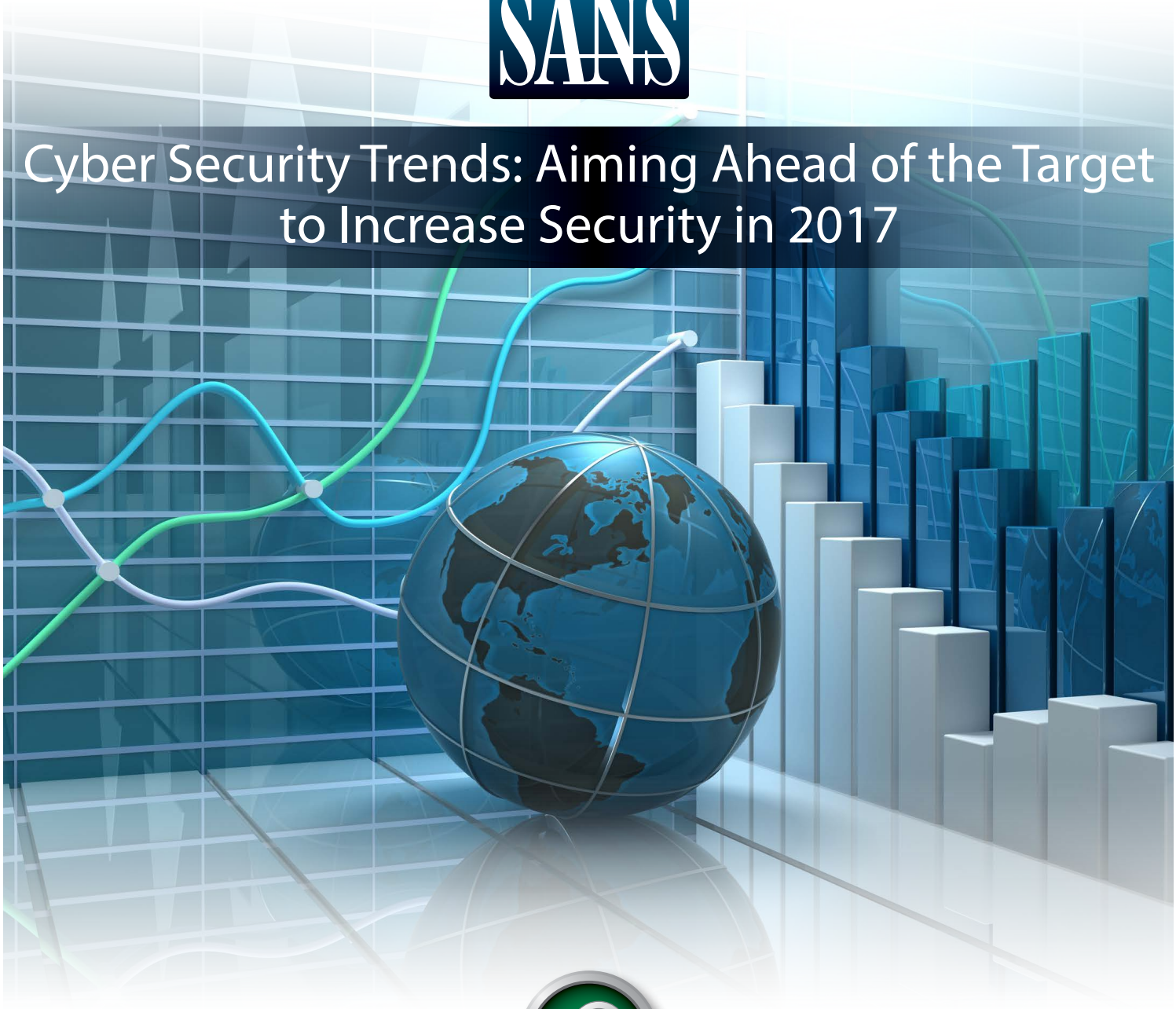
Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017



A SANS Whitepaper

Written by John Pescatore

March 2017

Sponsored by
Qualys

Introduction

In security, change always equates to risk. Because change is constant, being aware of the key changes that will increase risk is a critical part of being proactive in cyber security. A simple equation for risk is the following:

Threats are malicious tactics and techniques that would cause damage to a business.

Vulnerabilities are weaknesses that enable those threats to succeed.

Action consists of two components:

- Attacks that malicious actors (external or internal) take to launch threats
- Prevention or mitigation efforts by security teams to reduce the attack aperture or increase speed of detection

In reality, security teams control only half of the "Action" parameter. We can't determine when threats will be developed or launched, and vulnerabilities are driven by weaknesses in people and technology. People change slowly, but technology changes rapidly, and business adoption of new technologies invariably brings new vulnerabilities that enable new threats. Understanding and anticipating business demand for emerging technologies is a key element in successful security programs.

With each new wave of technology, threats tend to come in three forms: denial-of-service (DoS) attacks, cyber crime and attacks by nation-states.

DoS Attacks

When weaknesses in new technologies are exposed (generally by experimenters, academics and hacktivists), DoS attacks are the easiest to launch. They crash systems or cause data storms that bring networks to a halt.

Cyber Crime

Cyber criminals and the ecosystem that supports them refine attacks to focus on approaches that can lead to revenue, most commonly by stealing information that can be resold or support account fraud.

Attacks by Nation-States

Most, but not all, attacks launched by nation-states take advantage of the vulnerabilities exposed and techniques developed in the two earlier stages to develop highly refined and targeted attacks against specific targets of national value.

In all three cases, the underlying vulnerabilities that are exploited generally are not different. While reducing vulnerabilities is key to avoiding or minimizing damage from all forms of attack, what changes most significantly over time is the delivery mechanism for threats.

Changes in threats are only one factor that will impact cyber security programs. Changes in technology and business demand for using new technologies often cause much larger breakage to existing security processes and controls. This paper looks at the threat trends and business technology trends that cyber security teams should pay attention to in 2017 to help them focus their resources on the highest-payback areas.

Threat Trends

Three trends in the threat arena will be particularly relevant in 2017.

Known Vulnerabilities Will Continue to Dominate

While attacks that exploit zero-day vulnerabilities tend to get the most press coverage, data shows that attacks that exploit well-known vulnerabilities cause the vast majority of business damage. SANS estimates that over 80 percent of cyber security incidents exploit known vulnerabilities, and the annual Verizon Data Breach Investigation report shows similar numbers.[1] Gartner comes in much higher, estimating that "through 2020, 99 percent of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year."[2]

Due to business technology trends (discussed below), the quantity of zero-day vulnerabilities will increase simply because of the increasing number of products and operating systems that will be in use. However, the highest risks will still come from well-known and well-understood vulnerabilities. The key to reducing business damage is faster detection of vulnerabilities and more rapid and accurate mitigation. Where mitigation, such as patching or replacing legacy software, is not possible, shielding via intrusion prevention and application-layer firewall techniques is critical. At a minimum, systems with known vulnerabilities that host critical data should be required to be under continuous monitoring to enable faster detection of attacks and compromises.

Breaches Won't Be the Entire Story

Several years ago, attacks matured, going from experimenters and hacktivists causing DoS attacks to cyber criminals looking to steal customer and business information for the purposes of account fraud and other financial crimes. Nation-states followed, with investigations proving Chinese and United States intelligence agencies had perpetrated attacks.

The visibility of breaches caused many organizations to focus on monitoring databases and networks for signs of large quantities of data being exfiltrated to avoid or disrupt breach attempts. From 2015 to 2016, while the number of breaches increased 17 percent, the average number of records exposed per breach decreased by 82 percent as enterprises became more vigilant in detecting mass outflows of data.[3]

[1] "2015 Data Breach Investigations Report," Verizon, https://msisac.cisecurity.org/whitepaper/documents/1.pdf

[2] "Gartner's Top 10 Security Predictions 2016," June 15, 2016, www.gartner.com/smarterwithgartner/top-10-security-predictions-2016

[3] "Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout," Identity Theft Resource Center, Jan. 19, 2017, www.idtheftcenter.org/2016databreaches.html

However, criminals don't stay static. During 2015 and 2016, ransomware attacks showed high growth (see Figure 1).

Figure 1. Ransomware Is Spreading[4]

Find out more in SANS' Enterprise Survival Guide for Ransomware Attacks: www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962

Ransomware is really a form of DoS that uses malware to encrypt critical data or executables, thus bringing key business services to a halt. Ransomware attacks tend to exploit the same vulnerabilities as breach attempts, but they also exploit weaknesses in data backup processes and traffic monitoring.

A new form of ransomware that is sure to grow is called "badness planting." While badness planting takes advantage of the same vulnerabilities as other ransomware attacks, such attacks do not introduce malware to exfiltrate or encrypt data, but rather download onto corporate PCs and servers and compromise files, pictures or videos. By threatening to expose the planted content, the attackers either seek ransoms or, more insidiously, persuade users to provide their username/password credentials. As business users increase their use of social media and data centers expand their use of cloud services, this type of attack becomes easier to launch. The Cloudbleed vulnerability that Cloudflare recently exposed illustrates the changing nature of this risk.[5]

[4] "Kaspersky Security Bulletin 2016," https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf

[5] "Quantifying the Impact of 'Cloudbleed,'" https://blog.cloudflare.com/quantifying-the-impact-of-cloudbleed

Fourth-Party Attacks Will Increase

In 2013, Target suffered a breach that exposed over 40 million customer accounts and cost Target more than $100 million in direct costs. Attackers first targeted an HVAC contractor that had remote access into Target's stores and then exploited Target's weak network segmentation and monitoring. The Target breach increased the visibility of such third-party risks, but attacker trends continue to move outwards in the supply chain to include fourth parties such as subcontractors, outsourcers, cloud service providers and device manufacturers.

Assuring that third- and fourth-party services are secure enough for business use requires security teams to be involved in the supplier selection process and to have in place processes and controls to continuously monitor the vulnerability and compromise status of those business partners and suppliers.

In many ways, changes in threats are more manageable than changes in the increasing pressure for businesses to use new technologies and services. A new attack may or may not hit your organization, but when a security organization impedes new business initiatives, there's damage 100 percent of the time. Here are some of the strongest trends and how they impact security.

Mobility and Increased Use of Cloud Services

Businesses have been forced to change how they do business because of two important factors: the explosion of mobile devices, whether personal or company-owned, and the increased use of cloud services. For example, a 2016 Career Builder survey showed 83 percent of employees had smartphones at work, with two out of three using them multiple times per day.[6] IDC forecasts that by 2020, more than 70 percent of the workforce will be primarily mobile.[7] Businesses have seen clear benefits in cost savings and increased innovation by enabling mobility.

Along with those benefits, mobility has brought new risks. Mobile devices are heterogeneous, change rapidly and invariably bring along the use of external cloud services. This will add to the demand by business to use software- and infrastructure-as-a-service (SaaS and IaaS) offerings to reduce time to market and capital expense costs.

A 2017 study published by Skyhigh Networks showed that the average enterprise today uses dozens of business-approved cloud services, as well as hundreds of unsanctioned cloud services.[8] While this number is likely to decrease over the next few years as the overcrowded cloud services market shakes out, the amount of critical data flowing to cloud services and the level of business dependency on cloud services will only increase (see Table 1).

Table 1. Cloud Shift Summary by Market Segment[9]

Legacy segment	Cloud segment	Total market size in 2016	Total cloud shift in 2016	Cloud shift rate through 2020
Business process outsourcing	BPaaS	$119 billion	$42 billion	43%
Application software	SaaS	$144 billion	$36 billion	37%
Application infrastructure software	PaaS	$177 billion	$11 billion	10%
System infrastructure	IaaS	$294 billion	$22 billion	17%

BPaaS *= business process as a service;* ***IaaS*** *= infrastructure as a service;* ***PaaS*** *= platform as a service;* ***SaaS*** *= software as a service*

[6] "New CareerBuilder Survey Reveals How Much Smartphones Are Sapping Productivity at Work," June 9, 2016, www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F9%2F2016&id=pr954&ed=12%2F31%2F2016

[7] "Why You Should Care About Mobile Workforce Management," http://tech.co/mobile-workforce-management-2016-01

[8] "Cloud Adoption and Risk Report," Q4 2016, www.skyhighnetworks.com/cloud-report

[9] "Gartner Says by 2020 'Cloud Shift' Will Affect More Than $1 Trillion in IT Spending," July 20, 2016, www.gartner.com/newsroom/id/3384720

Increased use of cloud services breaks IT's traditional administration and operations processes, which impacts the security program's visibility and control capabilities. Essentially, every use of SaaS is like a new unique software application in use, and every use of IaaS is like a new data center being added—but without IT being able to dictate things such as version control, patch frequency and code reviews. Most IT organizations will be forced to update their development, QA, administration and operations processes.

As business demand forces IT to make the transition to cloud services, security organizations should make sure security controls are maintained or even enhanced. To reduce the risks of moving to cloud services, IT needs to extend to those services their security processes for continuous monitoring, vulnerability management and compliance monitoring. This includes doing the following:

- Assuring that the security team participates in the cloud service selection process and that security requirements are included and highly weighted among the evaluation criteria.
- Emphasizing configuration and application vulnerability assessment and mitigation as part of the development process and final QA before applications are approved for deployment onto cloud services.
- Integrating continuous monitoring for security vulnerabilities and changes into updated IT administration and operations processes as IaaS and hybrid cloud use grows.
- Merging the monitoring data from cloud services with that from applications hosted in the company's data center.

The increased use of cloud services will also extend to security services. Whenever IT adds a new delivery mechanism, security must add that same mechanism. Cloud-based delivery of security services has been increasing over the past few years, and that growth will accelerate. Hybrid architectures, where on-premises security controls are integrated with cloud-based security capabilities, will become the norm for all large enterprises and government agencies.

The Internet of Things

The Mirai attacks of 2016 proved that despite complaints that the Internet of Things (IoT) had been overhyped, real-world attacks exploiting IoT vulnerabilities were already causing real damage to real enterprises.[10]

Simplistically, the IoT consists of everything that has Internet connectivity. By that definition, growth in "things" has outstripped the adoption rates of every previous technology (see Figure 2).

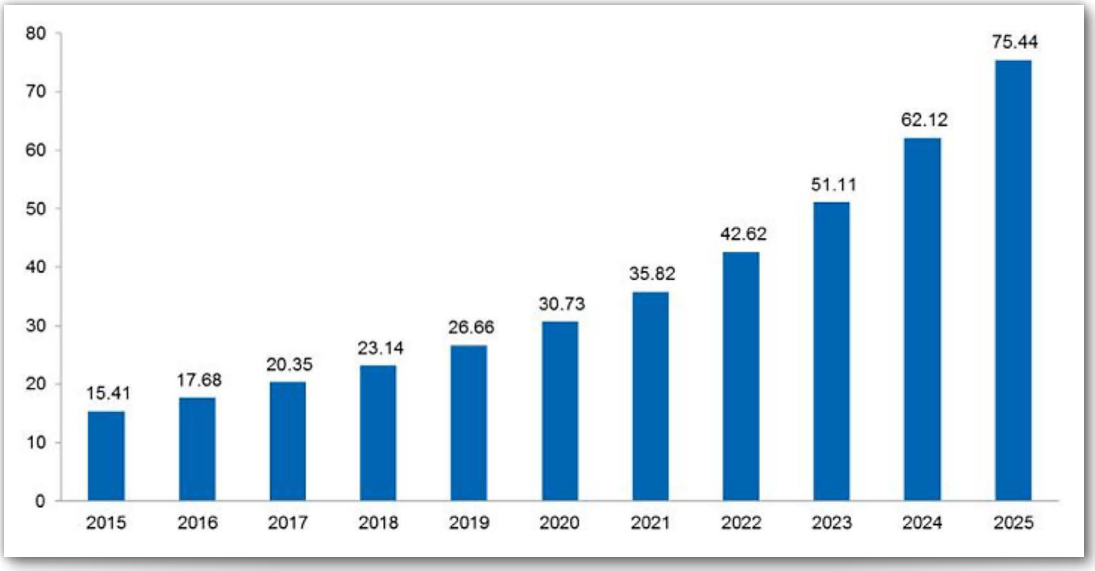


Figure 2. IoT Devices Expected to Quintuple in a Decade.[11]

However, from a security perspective, it is important to look at the different types of devices that make up the IoT. SANS defines four:

- PCs, servers, routers, switches and similar devices, primarily using wired connectivity, bought by enterprise IT
- Medical machinery, SCADA, process control, kiosks and similar technologies, primarily using wired connectivity, bought as appliances by enterprise operational technology (OT)
- Smartphones and tablets bought as IT devices by consumers (employees) exclusively using wireless connectivity and often multiple forms of wireless connectivity
- Single-purpose devices (whether bought by consumers, IT or OT) that exclusively uses wireless connectivity, generally of a single form

[10] "Port 7547 SOAP Remote Code Execution Attack Against DSL Modems," SANS ISC InfoSec Forums, https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759

[11] "IoT platforms: enabling the Internet of Things," IHS Markit, March 2016, https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

The first three types of devices are all in use today. As each type emerged, it caused tremendous security breakage and required security changes such as IT/OT integration, bring-your-own-device security controls, network access control and new forms of vulnerability assessment and management.

The growth over the next few years will be of the fourth type. These single-purpose devices are showing up embedded in infrastructure (smart buildings, smart cars, environmental monitors) used by enterprises, as well as in standalone products of every shape and form that employees (not just customers) will use and often connect to business networks. Security processes for discovering and managing familiar mobile devices running standard versions of iOS or Android are often blind to such embedded or single-purpose devices. The increase in heterogeneity will cause breakage in discovery, vulnerability assessment, and management controls and processes, which will enable attackers to use vulnerable "things" to launch all forms of attacks.

Board-Level Interest and Demands

The scope and visibility of Sony's breach in 2014 began a trend that will continue to accelerate in 2017 and beyond: Corporate boards of directors are increasingly pushed to pay attention to cyber security as part of their oversight roles. Before the Sony breach, 7 percent of directors considered cyber security to be a high priority. Driven in large part by the high visibility and the high level of business damage in the Sony breach, that percentage rose to 30 percent by 2016.[12]

SANS estimates that today, more than 60 percent of large-company CISOs brief the board at least annually. By the end of 2018, 70 percent of all boards will require CISOs to brief them quarterly. In addition to the publicly disclosed breaches driving this interest, regulatory bodies and Congress have begun to query corporate management and boards on their level of understanding and oversight of cyber security-related risk.

As a result of the closer attention being paid to security, board members will have high expectations about the quality and strategic value of the information they receive from CISOs. Boards expect the CFO to discuss high-level risks and financial strategies, and they take for granted that the finance department follows generally accepted accounting principles and basic financial hygiene. CISOs and security managers now are expected to provide the same level of strategic information to the board and to live up to expectations that tactical and operational issues, such as basic security hygiene, are addressed and are effective.

Thoughts from the Boardroom

Earlier this year, John Pescatore interviewed boards of directors and the CISOs who had briefed them across a wide range of industries. Some common themes came up:

- "CISOs are great on 'blood in the streets,' weak on strategy to avoid it."
- "CISOs don't speak our language—and seem to speak a different language each month."
- "The board is strategic, not tactical." ("Not an ATM machine.")
- "We expect to see CISOs present consistent metrics that are connected to business goals and prioritized by how much risk is presented to the bottom line."

The choice of metrics was dependent on the particular industry and organizational governance and culture, but a few operational security metrics were universal:

- Time to detect a critical vulnerability
- Time to resolve or mitigate a critical vulnerability
- Time to detect an incident
- Time to resolve a problem and recover and restore business operations after an incident

[12] "Improving The Security Conversation For CIOs, CISOs, & Board Members," DarkReading, Sept. 28, 2016, www.darkreading.com/careers-and-people/improving-the-security-conversation-for-cios-cisos-and-board-members/d/d-id/1327030

Constants = Better Blocking and Tackling

The trends that will impact security programs require new architectures, processes, controls and skills to maintain acceptable levels of cyber risk. However, just as losing weight invariably requires eating less and exercising more, there are some key areas of cyber security that should not change but provide the essential foundation for dealing with new risks.

Basic Security Hygiene

As pointed out earlier, the vast majority of successful attacks will continue to exploit well-known vulnerabilities—essentially exposing a lack of basic security hygiene. SANS has long supported the Critical Security Controls effort, which began at the National Security Agency in 2008 and is now a community effort coordinated by the Center for Internet Security (CIS). The CIS Controls have proved to be an effective framework for focusing security resources on effective and efficient security controls that present the highest barriers to real-world attacks.

The CIS Controls are updated periodically, with the latest version (6.1) released in December 2015 (see Figure 3).

Figure 3. CIS Critical Security Controls v6.1

The major changes include the following:

- "Controlled Use of Administrative Privileges" was increased in priority, moving from CIS Control 12 to CIS Control 5, recognizing the high number of attacks that were taking advantage of over-privileged accounts.
- "Secure Network Engineering," which had been CIS Control 19, was deleted because the key concepts of segmentation were covered in other areas.
- "Email and Web Browser Protections" was added as a new control, based on the high percentage of incidents caused by threats initiated by phishing attacks.

Subcontrols were grouped into one of three families—system, network and application—to aid in deployment planning and to clarify mapping to frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

By focusing on the first five CIS Controls, enterprises can build a strong foundation for dealing with the trends identified in this paper and mitigate or prevent many common security incidents.

Common Success Patterns

In 2016, the Identity Theft Resource Center documented 1,093 publicly disclosed breaches that exposed almost 37 million records.[13] That represents almost a 40 percent increase over 2015, but it also means 8,900 of the Fortune 10,000 companies avoided such breaches. While the number of breaches increased, the average number of records exposed per breach also declined significantly, from an average of over 228,000 records per breach in 2015. This indicates that many organizations managed to reduce the scope of breaches by being faster at detecting incidents and initiating mitigation.

Over the years, SANS has observed a number of success patterns common across businesses and government agencies that have avoided or minimized damages from all forms of attack. These include the following:

Mature foundational security is required before higher-level risks can be addressed—A mature security program has the ability to maintain its focus on basic security hygiene (as typified by the CIS Controls), both in the security program and in IT operations and business units. Effective and efficient resource visibility and vulnerability management processes not only prevent damage from simple attacks, but they also remove the low-value alerts that often cause noise and mask the signals of advanced targeted attacks.

Vulnerabilities are avoided by injecting security into software development, acquisition and supply chain processes—The least risky vulnerability is one that never makes it onto a product system, application or process. Extending continuous monitoring and vulnerability awareness and mitigation into software development/DevOps processes and into the evaluation and acceptance criteria for procured software and cloud services not only efficiently reduces attack surfaces, but it has been proven to reduce time to market for secure business services.

Force multipliers relieve the need for more staff—While there are numerous press reports of demand for hundreds of thousands of security practitioners, real-world budgets simply can't support doubling security staff levels. SANS has seen that the real demand is for high-level security skills, but often the security analysts with those skills are swamped with more routine tasks. Force multipliers are processes, tools and services that can enable less-experienced security staff to effectively deal with base-level security tasks, enabling those "security unicorns" to focus on more complex and higher-value actions.

[13] "Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout," Identity Theft Resource Center, Jan. 19, 2017, www.idtheftcenter.org/2016databreaches.html

Working effectively with IT operations for faster patching and mitigation is more valuable than simply doing more vulnerability listing—Most security budgets are consumed by operating security processes and controls to make up for deficiencies in IT operations: misconfigurations, failure to patch, over-privileged accounts, use of default passwords, etc. CISOs and security teams that can communicate and work proactively with IT operations to identify and address the root cause of vulnerabilities can reduce both risk and security spending at the same time.

Extending to the cloud requires securing the cloud from the cloud—As detailed above, the use of external cloud services will only grow. Businesses with the best track record in avoiding cloud-related security incidents have focused on extending their security architectures, processes and visibility into the cloud to have an integrated situational awareness view of risk, vulnerability and incident status. Taking advantage of security services delivered from the cloud has been one key element in enabling that integrated approach.

Summary

Many things never change in cyber security. The fundamental blocking and tackling of hardware/software inventory, vulnerability assessment and mitigation, governance and business continuity planning are not only still important, but they are also the essential foundation for any security program to efficiently and effectively protect critical data from advanced threats and enable the business to safely use new business processes and technologies.

However, in technology in general and cyber security in particular, change will continue to be a constant. Cyber criminals and other attackers will continue to develop new threat vectors. Even more importantly, and more rapidly, new technologies and new demands by businesses to use those technologies will threaten to break even the most secure foundations. Increased demand for use of cloud services and new "things" are the major examples of those trends today.

Many cyber security programs have been successfully balancing those business demands with the dangers of new threats. The success patterns identified above have demonstrated techniques and tactics that the good guys can use to both stay ahead of the bad guys (or at least stay even) and to demonstrate to CEOs and boards of directors that their investment in cyber security both reduces risk overall all and enables the business to exploit those new technologies while keeping customers safe.

About the Author

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTA, and service with both the National Security Administration, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems "and the occasional ballistic armor installation." John has testified before Congress about cyber security, was named one of the 15 most influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this paper's sponsor:

QUALYS®