A SANS Whitepaper

Breach Avoidance: It Can Be Done, It Needs to Be Done

Written by **John Pescatore**

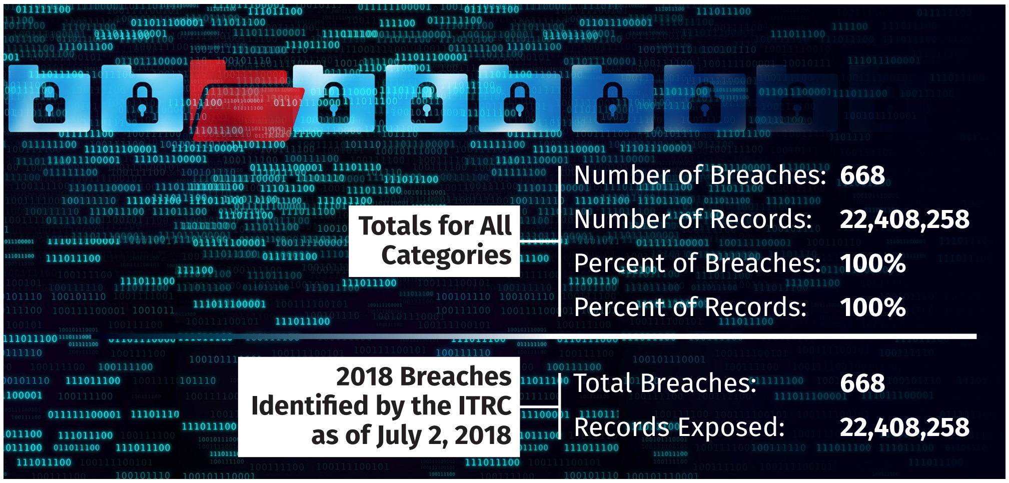
September 2018

Sponsored by:

Balbix

Despite the Hype, Most Breaches Are Avoidable

There is no shortage of horror stories about cybersecurity. Almost daily the press reports yet another exposure of sensitive business and customer information, or business outages caused by ransomware or denial of service attacks. While the press and security consultancies thrive on successful breaches, successful businesses thrive on avoiding as much downtime as possible and demand that their cybersecurity investments support that goal. In fact, the Identity Theft Resource Center (ITRC) reports that in the first 203 days of 2018 there were 668 publicly disclosed breaches in the United States.[1] At this rate, more than 1,200 breaches, or more than three per day, will occur this year. See Figure 1.



Totals for All Categories	Number of Breaches:	668
	Number of Records:	22,408,258
	Percent of Breaches:	100%
	Percent of Records:	100%
2018 Breaches Identified by the ITRC as of July 2, 2018	Total Breaches:	668
	Records Exposed:	22,408,258

Figure 1. Publicly Disclosed Security Breaches in the First Half of 2018

[1] "Identity Theft Resource Center: 2018 – Data Breach Summary Category," www.idtheftcenter.org/wp-content/uploads/2018/07/ITRC-Breach-Stats-Report-Summary-Y-T-D-2018.pdf

On a positive note, this statistic also means that many businesses will manage to avoid a significant breach this year. There are more than 18,000 companies with more than 500 employees in the U.S., meaning about 17,000 of them will have avoided a breach requiring disclosure in 2018. Some companies will simply be lucky enough not to be attacked or may suffer only minor incidents. Many more will avoid or limit business damage by implementing security processes and controls to proactively identify and remove or mitigate vulnerabilities.

The ITRC data also shows that while 2018 is on pace for roughly the same number of breaches as in 2017,[2] the total number of records exposed in 2018 is running 66 percent less than last year. While many companies don't detect incidents until customers complain (or the FBI calls!), others are detecting attacks in the early stages of the "kill chain" and are able to reduce the extent and cost of the incident.

The bottom line is that breaches are **not** inevitable. There are proven techniques in use today by large and small companies with limited staff and budgets that can fend off or avoid most attacks and dramatically reduce the damage of attacks that do succeed. For example, organizations that emphasize proactive security efforts to reduce vulnerabilities in critical business assets are less likely to suffer major business damage than organizations that don't have the skills and tools to prioritize and focus security efforts. Successful security programs rely on more than just faster incident response to take on the challenge of damage avoidance and reduction. This paper will detail the success patterns SANS has witnessed by security programs doing just that.

Action Is the Magic Ingredient in Breach Avoidance

Although there are many complex risk assessment and management frameworks, one simple risk equation has proven to be true over the years:

Risk = Threats x Vulnerabilities +/– Action

Security teams don't control the threats. Attacks will always occur—on the attacker's schedule and using increasingly sophisticated delivery mechanisms and evasion techniques.

People and software will always have **vulnerabilities**. While there are actions we can take to avoid some vulnerabilities and mitigate many others, the reality of phishing and patching tells us that new vulnerabilities will always be discovered.

> *"99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident."*
>
> —Susan Moore, Smarter with Gartner[3]

We don't control the **risk-increasing (+) aspect of action**. Risk increases when attackers launch and refine their attacks or when weaknesses in IT operations lead to misconfigured or vulnerable systems and applications.

[2] "2017 Data Breaches," www.idtheftcenter.org/2017-data-breaches

[3] "Focus on the Biggest Security Threats, Not the Most Publicized," November 2, 2017, www.gartner.com/smarterwithgartner/focus-on-the-biggest-security-threats-not-the-most-publicized

What we can control are the **risk-reducing (–) action components** of the risk equation. The key is for security teams to understand business impact, be able to express risk in those terms and be able to demonstrate how improvements in security result in measurable reduction in business impact. By developing situational awareness (timely and accurate knowledge of what we need to protect, what vulnerabilities exist, and what real threats are active against those targets), and combining it with tools and techniques for prioritizing prevention and mitigation actions, security teams can quickly take actions to avoid the most damaging incidents and to exponentially reduce the business damage of unavoidable incidents.

> *We don't control the risk-increasing (+) aspect of action. What we can control is the risk-reducing (–) action components of the risk equation.*

The Right Proactive Actions Are Key—Not Just More Activity

"Defense in depth" is an overused phrase in cybersecurity. It generally really means "spending in depth"—in other words, keep doing what you were doing, but add more security products and services, which invariably increases cost and complexity. While many security programs are underfunded, over the years there has been minimal correlation between the level of security spending and the level of business damage caused by security incidents. There are several reasons for this:

- Simply adding layers of security products increases complexity, requires security staff skills that are hard to find and often results in more disruption to business operations than to attackers.
- The enterprises with the lowest levels of damage almost invariably are the ones with strong security teams that avoid the most vulnerabilities by proactively driving change in IT operations and procurement to minimize vulnerabilities and misconfigurations in IT systems and applications.
- Because it is impossible to avoid all vulnerabilities, prioritizing staff resources and procurement of security products and services to address the areas of highest risk first and most frequently is key to both effective and efficient cybersecurity.

To address continually evolving threat scenarios and real-world budget and staffing constraints, well-defined and integrated security processes, backed by "force multiplier" tools, are needed. See Figure 2.

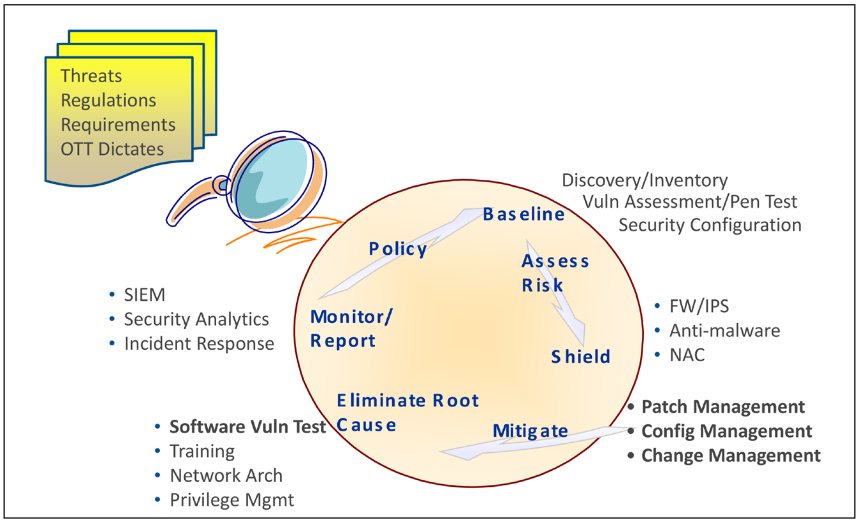


Figure 2. Examples of Integrated Security Processes[4]

[4] "DevSecOps – Building Continuous Security Into IT & App Infrastructures," October 2017, www.sans.org/webcasts/devsecops-building-continuous-security-app-infrastructures-105665/success, webcast presentation slide 7. [Registration required.]

These processes are well-known, and many enterprises can point to where all these functions are being performed. However, the most effective and efficient security programs have the "arrows" shown in Figure 2 connecting the processes—documented and functional interfaces and procedures that integrate individual security controls and actions into repeatable and adaptable security processes. These processes, combined with investments in the skills, tools and techniques, deliver on accurate baselining, streamlined risk assessment, and flexible shielding and mitigation approaches.

Focusing on these core processes is critical for increasing the number of avoidable or minimized security incidents. Incident response processes are important and will always be essential, but the most cost-effective way to minimize business damage is to avoid breaches as much as possible.

Success Patterns for Breach Avoidance

One of the difficulties with cybersecurity is that the environment and constraints differ by industry, geography, company size and corporate governance/culture. However, SANS has recognized some key success patterns common across enterprises that have been able to avoid more breaches and that do the best job of minimizing business damage overall.

Key Success Patterns

- Choosing a cybersecurity framework that prioritizes by real-world risks
- Instituting continuous monitoring of assets
- Mapping against real-world threats
- Developing and updating "playbooks" that incorporate tool support and automation

Using a Cybersecurity Framework to Prioritize "Protect the Business"

The majority of damaging breaches have occurred to enterprises that one or more auditors judged to be "compliant." But compliance does not equal security—it simply means that a single-point-in-time assessment (often questionnaire-driven) against general-purpose criteria resulted in no observable deficiencies. Simply achieving compliance can avoid some level of fines, but it does not assure actual protection of business and customer information, nor has it even been shown to provide any legal cover or liability reduction if incidents do occur.

The use of a cybersecurity framework that prioritizes actions and controls by business risk is key to focusing on what security processes and controls are the most important to avoid incidents that would disrupt business operations or expose customer information. While compliance standards include every possible security control that can be utilized, good frameworks enable prioritizing and integrating actions to focus resources on the areas most likely to reduce business damage. Examples of cybersecurity frameworks that are in use to support business protection and risk reduction include:

- NIST Cyber Security Framework
- CIS Critical Security Controls
- PCI Data Security Standards Prioritization Guidelines
- Health Information Trust Alliance (HITRUST) Common Security Framework

Instituting Complete, Accurate and Prioritized Continuous Monitoring

You can't protect what you don't know is there. Knowing what systems, applications and data are in use by the business and having accurate and timely information on vulnerabilities because of missing patches, misconfigurations or other security gaps enable proactive efforts to mitigate or shield systems before attacks are launched.

Periodic vulnerability scanning may be compliant, but it's almost never sufficient. The use of a mix of network-, host- and credential-based assessment tools on a continual and automatic basis is generally required to assure completeness, accuracy and "freshness" of inventory and vulnerability data. Security professionals need similarly fresh knowledge of business operations mapped to IT assets to ensure that current and accurate risk assessments cover all critical systems.

Mapping Against Real-World Threats and Business Context

Invariably, mature cybersecurity asset inventory and vulnerability management processes produce large volumes of vulnerability alerts. Simply converting those alerts to trouble tickets may satisfy auditors but in practice simply overwhelms IT operations staff with what they consider to be low priority requests.

When vulnerabilities are mapped first against active threats that exploit those vulnerabilities and then by criticality to business operations, security teams have been able to justify the need to take immediate patching, reconfiguration or shielding actions. To deal with limited personnel skills and availability, tools that support or automate analysis can be leveraged to prioritize actions by risk.

Using Updated "Playbooks" for Damage Avoidance

The term *playbook* has generally been associated with incident response processes where techniques and procedures are documented to ensure that actions taken after the detection of an incident are repeatable and complete. Playbooks essentially capture the knowledge of a skilled security analyst and document the steps that expert would take. That same concept has proven effective for exposure reduction, breach avoidance and damage minimization.

For static events, repeatable playbooks that recommend mitigation and shielding steps based on asset criticality and threat classification can allow lesser-skilled analysts to take steps to reduce risks while the hard-to-find "unicorn," the highly skilled analyst, focuses on unique or crisis-type events. Threats change constantly, and the rate of change of business needs also results in a high level of volatility in IT systems and software. Dynamic playbooks are needed to stay in sync and maintain accurate risk assessment and prioritization of actions across changing conditions.

Metrics for Success

An often-overlooked factor is the ability to show the CIO/CEO/board of directors what the current level of risk looks like and how efficiently and effectively security program investments are being strategically deployed to control and, hopefully, reduce risk over time. The most effective security programs develop processes and methodologies to provide high-level views of risk that are understood by management even though they are derived from data that is used by both security and IT operations for tactical decision making.

For security operations, SANS has identified three key operational metrics as mandatory to meet the preceding goals of both risk tracking and security operations improvement:

- **Time to detect.** This is traditionally the time between when an attack first touches an asset and when a security incident is declared.
- **Time to respond.** For attacks that do get through, prioritized actions can reduce both the time to deal with an evolving incident and the damage caused by the attack and any response actions.
- **Time to restore.** The real measure of a successful security program is minimizing any business disruption. Prioritized actions based on the details of the threat and the criticality of the business asset, as well as dynamic and specialized playbooks, are key to this outcome. Security programs that focus on breach avoidance reduce time to restore to **zero** for as many attacks as possible.

Risk Posture over Time

The three "time to" metrics discussed above have proven critical to measuring and increasing the efficiency and effectiveness of a security operations center (SOC). Higher-level metrics and measurements are needed to manage the overall security program, and for effective presentation to the C-suite and the board of directors.

Examples include showing time series of the level of risk exposure of critical business systems that decline over time because of faster patching or shielding, improved basic security hygiene (such as stronger authentication or improved configuration rigor) or improved focus on avoiding software vulnerabilities. Trend analysis of threats, vulnerabilities and business impact allow CISOs to demonstrate success, as well as document lessons learned from failures, and support justification for the overall strategic cybersecurity approach and any necessary tactical actions. The capability to make near-term predictions and take proactive mitigation steps based on new threats or new vulnerability information supports being proactive in avoiding the conditions that would lead to business damage—the equivalent of "pulling the red handle" on a production line the moment that possible defects are discovered.

> *Demonstrating to management that the security program has a proactive and strategic approach to effectively reducing risks by efficiently deploying people and products allows CISOs to gain the trust of management, which leads to backing needed changes.*

Though it is often difficult to achieve, the overall goal for a cybersecurity program should be to demonstrate that investments in the cybersecurity program are directly linked to reducing the average business cost per attack. That cost includes both business disruption costs and security programs costs and will never reach zero—just as business line production costs never reach zero. The business goal is to always avoid as many "defects" as possible and rapidly and efficiently address those that can't be avoided. Demonstrating to management that the security program has a strategic approach to effectively reducing risks by efficiently deploying people and products allows CISOs to gain the trust of management, which leads to backing needed changes.

Framework: Focus on the First 6 CIS Critical Security Controls

As mentioned earlier, using a security-oriented framework (versus one that is compliance-oriented) is part of the success patterns observed over the years. SANS has long been a backer of what is now known as the Center for Internet Security (CIS) Critical Security Controls. The CIS Critical Security Controls[5] are based on a community effort to analyze how real-world threats are succeeding and to prioritize those security controls that are the most effective in disrupting real-world attackers.

Basic CIS Controls

1. **Inventory and Control of Hardware**
2. **Inventory and Control of Software Assets**
3. **Continuous Vulnerability Management**
4. **Controlled Use of Administrative Privileges**
5. **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**
6. **Maintenance, Monitoring and Analysis of Audit Logs**

Figure 3. Basic CIS Critical Security Controls

The first six CIS Controls essentially represent "basic security hygiene" (see Figure 3), and studies have shown that the vast majority of real-world attacks can be defeated when these controls are implemented effectively.

The six basic CIS Controls form the basis of the following guidelines for security hygiene:

- **Know what you are protecting.** Controls 1 and 2 focus on complete and accurate inventory of what devices, operating systems and applications are in use by the business. To maintain accuracy, discovery needs be performed in real time and continually, including across cloud, mobile and IoT assets.
- **Continuously monitor vulnerability of resources.** Control 3 emphasizes timely and accurate assessment of which assets are vulnerable to known and active attack vectors. Vulnerability assessment needs to be much more comprehensive and frequent than checking for Windows patches on a monthly basis—increased use of mobile and IoT devices has resulted in a much more heterogeneous mix of operating systems and applications with widely varying vulnerability announcements and patch releases.

[5] "CIS Controls," www.cisecurity.org/controls

- **Limit and monitor administrative privileges.** The vast majority of attacks require installing malicious software or obtaining high-level access rights to data to succeed. Control 4, which emphasizes monitoring and controlling admin rights, has proven to be highly effective in avoiding breaches.
- **Maintain secure configuration baselines.** Control 5 focuses both on having defined secure configuration baselines for each asset type and on active capabilities to restore misconfigured assets to safe configurations.
- **Implement continuous monitoring and situational awareness.** Control 6 is pretty straightforward, but also focuses on prioritizing actions based on collected data.

The Australian Signals Directorate (ASD, Australia's equivalent of the NSA in the U.S.) has based its cybersecurity improvements on a similar set of "basic" security controls that it calls the "Top 4 Strategies to Mitigate Targeted Cyber Intrusions."[6] The ASD has made these controls mandatory and demonstrated that their implementation has avoided damage from 85 percent of advanced targeted threats.

Prioritized and Proactive Action

Each year SANS conducts various surveys of the security community. Invariably, respondents have cited the top obstacles to security progress as limited budgets and the inability to hire enough skilled people.[7] However, successful security programs (like successful business line managers, who face similar real-world constraints) develop techniques for prioritizing investments in security controls, staff and tools to minimize business damage by avoiding as many incidents as possible and rapidly and surgically reducing the damage from those that do get through.

Tony Sager, CIS director for the Critical Security Controls, calls this dealing with the "Fog of More"—the need to prioritize actions to areas where most critical business assets can show the highest reduction in risk.[8] In the real world, resources are always limited, and the difference maker is the ability to prioritize and focus on the areas where proactive efforts will be the most effective. After all, security programs are paid to protect the business, not monitor and report on business disruption. Timely and appropriate action differentiates successful security programs from programs that are in the news for breaches.

In cybersecurity, accurate knowledge of vulnerability status can be combined with timely updates on emerging threat conditions to make rapid adjustments in prioritization, which can help the business be proactive in taking defensive steps before targeted attacks are even launched. Processes and tools to support this prioritization and

[6] https://acsc.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

[7] "2018 Endpoint Survey: Endpoint Protection and Response: A SANS Survey," www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460 [Registration required for access.] and "CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey," www.sans.org/reading-room/whitepapers/analyst/cti-security-operations-2018-cyber-threat-intelligence-survey-38285 [Registration required for access.]

[8] "The Fog of More: The Challenge of Simplifying Security," www.healthprivacyforum.com/sites/healthprivacyforum/files/the_fog_of_more_-_the_challenge_of_simplifying_security.pdf

proactive mitigation act as "force multipliers," effectively deploying scarce resources to focus on avoiding real-world threats that could compromise critical business activities. As previously discussed, each year incident investigations point out that the vast majority of security breaches could have been avoided if efforts had focused on ensuring basic security hygiene for critical business systems in a timely manner. While the press and security consultancies thrive on successful breaches, successful businesses thrive on avoiding as much downtime as possible and demand that their cybersecurity investments support that goal.

Summary

In every business, market conditions are risky and resources are limited. Successful businesses identify, predict and manage risk and deploy their resources based on prioritized strategies created from accurate business and market data.

Successful cybersecurity programs are following a similar path. The basic security processes and controls needed to identify, mitigate and shield vulnerabilities are well known. There is no shortage of information on threats and attacks. To succeed within real-world constraints of budget and staffing, cybersecurity managers need to focus first on integrated processes that can keep up with both the speed of business and the rapid evolution of attacks and then implement "force multipliers" to support accurate and timely prioritization of security resources. By focusing resources on protecting the most critical business assets against the most damaging potential threats, security programs can avoid many breaches and drastically reduce the business impact of any that do occur.

Resources

The resources provided here have been compiled from this paper to provide additional understanding about how to avoid breaches or minimize their impact.

"2018 Endpoint Survey: Endpoint Protection and Response: A SANS Survey"
www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460

"CIS Controls"
www.cisecurity.org/controls

"CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey"
www.sans.org/reading-room/whitepapers/analyst/cti-security-operations-2018-cyber-threat-intelligence-survey-38285

"Focus on the Biggest Security Threats, Not the Most Publicized"
www.gartner.com/smarterwithgartner/focus-on-the-biggest-security-threats-not-the-most-publicized

"The Fog of More: The Challenge of Simplifying Security"
www.healthprivacyforum.com/sites/healthprivacyforum/files/the_fog_of_more_-_the_challenge_of_simplifying_security.pdf

"Identity Theft Resource Center: 2018 – Data Breach Summary Category"
www.idtheftcenter.org/wp-content/uploads/2018/07/ITRC-Breach-Stats-Report-Summary-Y-T-D-2018.pdf

"Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained"
https://acsc.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

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, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, 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 cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this paper's sponsor:

Balbix®