WHITEPAPER

Learning from a breach

How security breaches happen—and how to stop them in their tracks.

Breaches are on the rise

Today, many IT and business leaders cannot confidently claim their organizations are safe from security breaches. While it's always preferable to prevent a security breach from occurring, it can be invaluable to learn from successful breaches.

For global security breaches, 2017 was an exceptional year. Consider these figures from the Ponemon Institute's Cost of Data Breach Study:

- Average total cost of a data breach: $3.62 M[1]
- Average cost per lost or stolen record: $141[1]
- Likelihood of a recurring breach over the next two years: 27.7%[1]

This white paper explores how and why breaches commonly occur. Then, it prescribes an approach that can help safeguard against the most common vulnerabilities.

Within the U.S., we saw many high-profile breaches:

- Credit rating agency Equifax was hit by a breach that affected as many as 143 million consumers[2]
- Uber, the online transportation technology company, revealed a hack that resulted in the theft of personal information from 57 million Uber riders worldwide[3]
- A breach at the CIA resulted in thousands of documents exposed and published on WikiLeaks, many of which were classified[2]
- The records of up to 14 million Verizon subscribers were discovered on an unprotected server[2]
- Travel technology company Sabre suffered an attack that exposed the reservation data of hundreds of airlines and thousands of hotels[2]

WINDSTREAM ENTERPRISE

The anatomy of an attack

Understanding how breaches occur is the first step to preventing one. Most successful attacks are committed in one of three ways:

1 Exploit an application-layer vulnerability

Hackers infiltrate a website designed to take in information, such as personally identifiable information (PII) data from a credit card, using malware or other means.

2 Use social engineering or a targeted attack

Hackers attempt to get an individual to grant access to an account within a system to expose personal information. Once they get into a single system or account, they can access the entire network, and other systems and accounts, systematically.

3 Enter through trusted third parties

Hackers target those who provide services to a company, then use that organization's network to gain access to the initial organization's data.

Attacks can vary by industry

Inside a healthcare data breach

Hackers execute their attack in one of the three ways outlined, setting their sights on high-value data, such as protected health information (PHI).

Breaking down a retail data breach

1. Hackers use an email phishing technique to steal a retailer's network login credentials from a third-party contractor.
2. They then use the stolen credentials to access the retailer's network via VPN.
3. From there, hackers map out the victim's internal network, then find and infect a vulnerable server.
4. Hackers use the infected service to distribute credit card collecting malware to the retailer's point of sale (POS) systems.
5. Malware copies credit card data from the POS system and transmits it to servers controlled by the hackers.

Taking apart a financial services breach

1. Cybercriminals send spoof emails from well-known social media or ecommerce sites alerting the recipient to a potential security threat.
2. The email encourages the recipient to visit a spoofed social media or ecommerce "Security Reset" page, where they validate themselves using their username and existing password and create a new password.
3. The recipient receives a legitimate email from the real site confirming the password change.
4. The hacker then accesses the actual site using the existing username and password and changes the password to match the new password captured on the spoof site.
5. The hacker uses the login credentials to commit identity or credit card fraud.

Multi-pronged attacks

Another tactic seen across industries includes the threat techniques described above combined with a dedicated denial of service (DDoS) attack, in which a company network is overwhelmed by superfluous requests. While the interruption may seem disconnected from other threats, hackers can use a DDoS attack as a smoke screen to distract an organization's IT resources and gain entry through a previously identified area of vulnerability.

Why security breaches occur

In today's increasingly cloud connected world, businesses digitally interact with their customers and partners more than ever. While there are obvious benefits, this also means they are more exposed to threats and vulnerabilities that allow cybercriminals to access critical systems and data. Some of these vulnerabilities are the result of human nature and can be avoided.

Password selection is an important issue. Consumers and business people alike make poor password choices, choosing ones that are easy to guess and crack. For example, since 2011, the top two passwords on the Internet were "123456" and "password," followed by "12345," "12345678," and "qwerty."4

Similarly, people are vulnerable to psychological manipulation and social engineering techniques that prey upon human emotions. To that end, many attacks are camouflaged as legitimate emails or other forms of official communication. Increasingly, hackers are posing as a company executive sending an email to an employee with a demand that funds be transferred to an account. By providing just enough information to convince someone in the company that they are executives, cybercriminals are granted access to sensitive data and systems.

Retailers are particularly vulnerable, as they deal with a tremendous volume of credit card information that is often distributed among many locations. Moreover, they often have inadequate staff and safeguards in place, so it can take months to detect a breach after it's happened.

In the healthcare industry, incentives for using electronic health records (EHRs) and the growing use of mobile devices mean PHI is more accessible than ever. Because they tend to prioritize improvements in patient care over infrastructure upgrades, healthcare companies lag behind their peers in other sectors. Without log management, reviews and alerts, attacks can easily go unnoticed.

All of which makes data theft big business. Complete identity theft kits—containing health insurance credentials, birth dates, Social Security numbers, addresses, and other personal information—can be worth up to $1,000 or more on the black market.

Typical breach/remediation timeline

Breach remediation is costly and can take months.
And that's not counting the potential long-term damage to a business' reputation.

Day 1

- Notify about breach
- Stop taking credit cards
- Pay for a forensic audit
- Monitor media/social media

Day 5

- Complete forensic audit
- Contact a Qualified Security Assessor (QSA)

Day 7

- Obtain proposals for remediation

Days 10–180

- Execute remediation and compliance plan
- Replace credit cards
- Disclose breach/address brand and media impact
- Post breach plus one year revenue impact

How companies can prevent breaches

The following steps may reduce the risk of a security breach occurring as described in the above scenarios.

Implement an application security program
Ensure all applications are written securely to eliminate flaws that lead to security breaches. That includes making sure to apply updates as soon as they are available from third-party software providers. Also, educate software developers, test during the software development life cycle and develop the secure coding standards used in current software writing.

Benefit/impact: Protects against web application hacking and internal application hacking attempts.

Identify valuable information assets across the company
A major part of the security battle is knowing what the organization is trying to protect and where it might be exposed or out of compliance.

Benefit/impact: Identifying critical assets provides a company with targeted security and risk investments.

Deploy perimeter security Managed firewalls, vulnerability scanning, and PCI-compliant WiFi keep data protected inside an organization's network.

Benefit/impact: The best defense is a proactive, layered approach of complementary, overlapping protection that is independent of other defensive measures.

Detect early Mandate 24/7 network-based intrusion detection, vulnerability scanning at all network levels, and continuous log monitoring and management to help detect and prevent threats before they become problems.

Benefit/impact: Continuous monitoring of threats enables early detection and proactive mitigation.

Be proactive A web app firewall at the application layer can detect and automate proactive countermeasures.

Benefit/impact: Web application firewalls provide a complementary control to secure application development but don't replace writing secure application code.

Enforce compliance Whether it's the Payment Card Industry (PCI) standard for merchants, the Health Insurance Portability Accountability Act (HIPAA) for healthcare, the Gramm-Leach Bliley Act (GLBA) for financial services or the Federal Information Security Management Act (FISMA) for government agencies, every industry has its own stringent regulations and standards. It's critical that organizations within each of those industries enforce compliance according to their respective standard.

Benefit/impact: Adhering to industry compliance standards helps protect the organization from potential legal challenges.

Vet third parties Third-party partner, supplier or customer access to an organization's systems, networks and data creates a potential attack vector. Make sure their security measures are aligned with your organization's, and that the other organization has a security program in place. In addition to surveying these third parties, make an onsite visit to verify they are truly practicing what they claim.

Benefit/impact: By transferring business functions to a third party, organizations are not transferring the risk, so it's critical to validate their security measures.

Educate everyone about situational awareness and phishing
Train the entire workforce, suppliers and even customers to be suspicious of unsolicited emails, social media posts and links. Keep them informed about phishing attacks, safe computing practices and other security trends. Also, teach them to be vigilant about proper WiFi procedures, leaving their laptop screens exposed to onlookers in public places, or unfamiliar people asking questions about office hours and company procedures. Encourage them to ask questions if they're being asked to do something that violates standard practices or general accounting principles.

Benefit/impact: Keeping users updated and informed about hacker trends and techniques translates into safe computing practices both in their personal and professional lives.

Make DDoS protection part of a broader strategy
Since IT budgets may be static, some organizations may neglect to cover all the bases even though security challenges continue to escalate. Be sure not to leave DDoS protection off the critical security list. Instead, look for solutions that cover both monitoring and mitigation, which brings it within reach for any size organization.

Benefit/impact: As attacks continue to grow in size and frequency, proactive monitoring, notification, attack verification and swift mitigation helps ensure the organization is protected.

Create a vigilant enterprise security environment

As hackers, criminal networks and malware become more sophisticated and aggressive, it's only a matter of time until a business experiences a serious security attack.

In the event that a breach occurs and results in the loss of sensitive information, the consequences could be serious—from fiscal, legal, and even public relations and business/brand reputation standpoints. Damage to the latter can amplify the direct monetary cost many times over.

In the current hyper-connected technology and media environment, it's not enough to satisfy security and compliance requirements. Organizations need to clearly understand their security risks, be prepared to protect and prevent damage to their most valuable assets, and isolate and respond to threats as soon as they appear.

1. Ponemon Institute. "2017 Cost of Data Breach Study: Global Overview." June, 2017. Sponsored by IBM Security.
2. ZDNet. "2017's biggest hacks, leaks, and data breaches—so far". Source: http://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2017. Zack Whittaker. September 20, 2017
3. ZDNet. "Uber concealed hack of 57 million accounts for more than a year." Source: http://www.zdnet.com/article/uber-concealed-hack-of-57-million-accounts-for-more-than-a-year. Zack Whittaker. November 21, 2017
4. Ponemon Institute. "Data Risk in the Third-Party Ecosystem, April 2016." As cited in Windstream. "PCI Compliance: Protect your business from a data breach."

About Windstream Enterprise

Windstream Enterprise collaborates with businesses across the U.S. to drive digital transformation by delivering solutions that solve today's most complex networking and communication challenges.

To learn more, visit windstreamenterprise.com

WINDSTREAM ENTERPRISE

CONNECT. TRANSFORM. ELEVATE.