GAINING TACTICAL AWARENESS &

NULLIFYING CYBERTHREATS

How CIOs Can Prevent and Withstand a Cyberattack

ConRes
IT SOLUTIONS

INTRODUCTION

From ISIS backers to disgruntled employees and Bring Your Own Device (BYOD), security breaches have become more sophisticated and frequent. In fact, according to the Breach Level Index, data breaches worldwide and the amount of information being stolen has increased dramatically. This includes nearly three billion data records that were either lost or stolen last year, representing a 71 percent increase compared to 2013.[1]

The purpose of this guide is to help you protect your most critical data from compromise. This includes how to:

- Identify potential vulnerabilities
- Develop a comprehensive data breach prevention plan
- Understand how IBM data security solutions can help protect your most critical data from compromise

1. http://www.breachlevelindex.com/#!home

CHAPTER 1: THE AGE OF DATA BREACHES

The cost of a data breach to a company can range from $9.3 million to $16 million, according to Ponemon Institute's 2014 Cost of Cyber Crime Study: United States.[2] Another Ponemon Institute report, 2014 Cost of Data Breach Study: United States, stated the average cost of each compromised record increased from $188 to $201 over the last year.[3] Most of that money is spent on detection and recovery activities, followed by investigation and containment. Consequently, the longer it takes to resolve the breach, the more expensive it is.

CIOs need to accept the fact that it's no longer a question of if, but when their companies will be breached and start thinking differently when it comes to data security. Companies need to face the hard truth that data breach will come to their company at some point. To be in denial of this truth is to not accept reality. Security pro Kent Schneider, former international president and CEO of the Armed Forces Communications and Electronics Association (AFCEA), added his opinion to the state of affairs of data security, stressing that 2014 was a landmark year for data breaches, but 2015 could be even more significant.[4]

2. http://insigniamquarterly.com/wp-content/uploads/2015/01/INS-winter-2015-The-Boardroom.pdf
3. http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
4. http://www.prnewswire.com/news-releases/security-expert-predicts-four-critical-cyber-trends-for-2015-300011236.html

CHAPTER 2: FINDING AND PLUGGING LEAKS IN YOUR NETWORK

Data leak prevention and network security are the most practical ways for IT decision makers to identify potential vulnerabilities. Eliminating these leaks can often make the difference between a smooth-running business and massive data breaches that could damage a company's financial stability and reputation.

Preemptive threat mitigation solutions that protect your entire IT infrastructure must be put in place to identify potential vulnerabilities. IBM network security services and solutions protect endpoints, applications, systems, and networks. Their services leverage the latest vulnerability and threat intelligence from the IBM X-FORCE™ research and development team to identify network security threats and risks across your organization. In fact, IBM security intelligence helped reduce the over 91 million security events detected in 2013 in any one of their clients' systems to an average of 16,000 attacks—and under 110 incidents—for a single organization.[5]

5. Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014

CHAPTER 3: SECURING THE CLOUD WITH BEST PRACTICES

The cloud gives organizations of any size the ability to innovate at top speed. But when it comes to cloud security, most businesses feel there's no concrete platform in place with assurances of protecting data. Forrester's survey of 321 IT professionals involved in public cloud security found that only 18% of respondents believe the native security capabilities of cloud providers are sufficient for their implementation.[6] This makes responding properly to a large breach a significant challenge especially if you're unsure that your service provider can deliver adequate data security.

IBM® Security QRadar® Security Identity and Access Assurance (SEIM) helps users gain access to cloud resources, while also monitoring, controlling, and reporting on the identities of the systems. It also:

- Provides near real-time visibility for threat detection and prioritization
- Delivers surveillance throughout the entire IT infrastructure
- Reduces and prioritizes alerts to focus investigations on an actionable list of suspected incidents
- Delivers security intelligence in cloud environments
- Produces detailed data access and user activity reports to help manage compliance

6. Source: IBM Global Cloud Study 2013

CHAPTER 4: MOBILE MANAGEMENT AND SECURITY IMPLICATIONS

A 2014 survey from Tech Pro Research shows that the Bring Your Own Device movement is booming, with 74% of organizations either already using or planning to allow employees to bring their own devices to work.[7] Key findings include:

- Nearly three quarters of respondent companies permit or plan to permit BYOD.
- BYOD is in greater use among small organizations compared to larger businesses.
- The IT, and education industries are most likely to permit BYOD, while government is least likely.
- Security concerns were the most common reason why BYOD was ruled out by respondents.

With MaaS360, organizations can phase in BYOD and leverage their mobile security investments for different classes of users, departments, geographies, devices, and applications. Companies can also apply the technology approach that best meets their needs, all from a unified platform. MaaS360 provides IT teams a wide range of mobile security options to separate corporate and personal information across different categories of users, devices, data, and apps. This provides the flexibility to offer tiered or layered mobile security to address varied end user needs and IT security requirements.

7. http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/

CHAPTER 5: MITIGATING RISKS AND IMPLEMENTING STRATEGY

Critical data, such as customer information and intellectual property, is essential for the success of any business. Knowing where your data is stored and what you need to do to protect it is a big part of the battle to prevent breaches and make your company less vulnerable to theft.

Here are some tips to prevent data leaks:

1. Designate a specific person who can maintain up-to-date info on financial regulations, policies, and other important records
2. Understand how your online transactions work and know their weaknesses
3. Batch process sensitive data to make it efficient and safer
4. Identify intellectual property throughout your online presence
5. Run vulnerability management programs on your websites. If an outside expert currently performs monthly intrusion attempts to test readiness, also consider employing an alternative company to test your systems defenses once quarterly
6. Adhere to SLAs and secure any business-to-business data

After shoring up your defenses, use QRadar Incident Forensics to identify remaining weaknesses. This program allows you to quickly apply effective vision and clarity to resolve, remediate, or mitigate the malicious security incident. It's also a natural complement to QRadar SIEM, which can comb through reams of log events and netflows to uncover high probability security incidents.

CHAPTER 6: DEVELOPING A RESPONSE PLAN FOR BREACHES

Why should companies create a response plan? Because in a recent survey on Data Breach Preparedness from the Ponemon Institute, only 38% of respondents felt their organization was prepared for a data breach.[8] It's critical to be prepared for the worst. Having a breach preparedness plan in place can help you act quickly, prevent further data loss, avoid significant fines from mandates like HIPAA, and costly customer backlash.

Acting fast and strategically following a data breach can help you regain your security, preserve evidence, and protect your brand. Always collect, document, and record as much information about the data breach and your response efforts as soon as possible, including conversations with law enforcement and legal counsel. Any plan should include recording the date and time of the security breach, alerting anyone on your response team, and stopping additional data loss by taking any affected machines offline.

8. Source: "Second Annual Study on Data Breach Preparedness," Ponemon Institute, 2014

CONCLUSION

Critical data, regardless of the percentage a company may store, is vital to that organization's core functions. Each priority item should be guarded and tracked as if your company's survival hinged on it because in some cases, it may. A well-constructed data plan, no matter how comprehensive and detailed, is only as good as the team responsible for putting it into action. Consider contracting with a data breach resolution partner to benefit from their strategic expertise in preparing for a breach.

Sign Up for a Free Assessment

Interested in discovering more on how IBM Security Solutions can protect your critical assets? Reach out to one of our experts for a complimentary assessment and be ready to defend yourself against today's cyberthreats.

ConRes IT SOLUTIONS

Premier Business Partner IBM