Executive summary: Cybersecurity and data breach preparedness

Prepared by:

Daimon Geopfert, Principal, RSM US LLP
daimon.geopfert@rsmus.com, +1 312 634 3400

Jim Lepine, Director, RSM US LLP
jim.lepine@rsmus.com, +1 404 751 9070

Rob Havelt, Director, RSM US LLP
rob.havelt@rsmus.com, +1 312 634 3400

Andy Obuchowski, Director, RSM US LLP
andy.obuchowski@rsmus.com, +1 617 912 9000

April 2015

As hackers become more advanced and expand their reach and methods, organizations must increase their focus on cybersecurity. Just one incident can have significant financial, reputational and regulatory consequences, so businesses must make it difficult for hackers to penetrate and advance through their environment and resources. You must take action to reduce the likelihood of a breach, improve detection and response to an incident and begin recovery as soon as possible.

Several misconceptions exist when it comes to cybersecurity, including that your company may be too small to suffer a breach or that you may not have valuable data. The reality is that all information has value, even on a small scale. Your organization has something hackers can take advantage of or make money off of, even if it is harvesting email addresses or commandeering your bandwidth.

Attacks are typically carried out in four stages: infiltration, propagation, aggregation and exfiltration. You must deploy controls within your environment to mitigate breaches at each stage of the cycle. Many organizations focus resources at the infiltration stage, but attackers are usually most skilled in this area. Successfully defending your environment is typically tied to the strength of controls in the latter three phases.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

Security controls can be preventive, detective or corrective by nature; however, the three distinct disciplines each require their own focus.

Preventive controls

Preventive controls are designed to keep incidents from occurring and serve as a deterrent against unauthorized access. Unfortunately, organizations are typically too focused on preventive controls and too trusting of their perceived effectiveness. For a program to be truly successful, preventive controls must be implemented with a plan for them to fail.

Control effectiveness varies greatly depending on the nature of the attacker. Not all hackers are created equal; they have vastly different skill levels and motivations.

Many preventive controls focus on securing the perimeter, but with emerging features, such as cloud adoption, remote access and mobility, the concept of the perimeter is outdated. Attacks can occur in many ways, and preventive controls must expand beyond the typical network boundary. In fact, preventive controls can be deployed throughout your environment to impede attackers as they attempt to work through the process.

You cannot count on perimeter controls alone and must implement measures to stop an attack in progress once they fail. Controls, such as firewalls and anti-viruses, protect against infiltration. However, once infiltration occurs, an attacker becomes a malicious insider.

Organizations can help prevent unauthorized access through several measures, including:

- **Network controls** — Depending on your framework, you may be able to take advantage of network segmentation, internal firewalls and access control lists, network access control, proxy servers, configuration management and egress filtering.
- **Domain and password controls** — Password storage and transmission is as important as password policy, as legacy storage and transmission systems make passwords easy to intercept and crack. In addition, attempt to harden your operating system and disable functionality that is not necessary.
- **Access methods and user awareness** — Two-factor authentication can add additional security to passwords and reduce the risk of compromised credentials. Employees should undergo periodic training to increase awareness of common and emerging attack methods.
- **Application security** — Web application firewalls can implement a set of customized rules to identify and block many attacks. The secure software development life cycle provides a framework to incorporate and stress security over and above existing guidelines.
- **Data controls** — A data life cycle management program increases your data classification and storage capabilities. It is difficult to protect data without knowing what you have or where it is. Successful encryption strategies help obscure file content and discourage theft.
- **Host and endpoint security** — Anti-virus software is still useful to protect systems from known malicious software, and endpoint security can recognize harmful activity and enforce certain behavior guidelines. Malware gateways screen inbound traffic and can block potential breaches.
- **Vulnerability management** — A vulnerability management platform identifies, classifies, remediates and mitigates exposures on a constant or periodic basis. It is a cornerstone of an information security program, but can be insufficient without the right focus and scope.
- **Security testing** — A thorough testing framework is necessary to ensure that controls are functioning as expected. Your organization should develop models of specific threats to test the resilience of your controls.

Preventive controls will not stop all attacks, but they make the overall process more difficult for hackers. Effective preventive controls force attackers to work harder to infiltrate your environment and increase the probability of being detected.

Detective controls

Detective controls help to monitor and alert your organization of any malicious or unauthorized activity. They provide support for post-incident corrective controls by allowing you to understand the method by which the attackers gained access and any data they may have accessed or stolen. To be successful, detective controls must be applied with the value of the asset or data in mind.

Infiltration has typically been the primary focus of detective controls, focusing on what is outside the network, rather than what is inside. However, detective controls can be implemented at any stage in the attack life cycle to increase your data security. System log data and alerts can help you stop the hacker at each stage:

- **Infiltration:** An attacker is performing network discovery, reconnaissance and attempting to gain access to your systems. Logs and alerts help determine where the hacker is from, block further attempts and gather threat intelligence for later use.
- **Propagation:** Attackers have breached a system and have become malicious insiders. They are attempting to access systems or valuable data. Hackers are easiest to catch at this stage. Logs and alerts provide a wealth of useful information and help understand the scope of the attack.
- **Aggregation**: The attacker finds and interacts with various data stores, decides what to take and begins processes to move information out of your network. Logs and alerts can help you discover an incident before the data leaves. You may be compromised, but you can prevent a full breach. Your organization has a much better view of what was potentially seen, altered and moved.
- **Exfiltration:** The attacker is working to remove information from your system, typically changing methods as attempts are blocked and using encryption to their advantage. Logs and alerts can show if aggregated data actually left your network and provide data on the location and identity of hackers and how long they had access to the network. If you catch on quickly, you can limit the breach's scope.

Logging by itself is not a control; it's the content, deployment and monitoring of logs that serves as the control to protect your data. Logging and alerting can be very granular and must be more robust at different stages of attacks. For example, many organizations set up a log for failed logins when implementing a server. That information is valuable at the infiltration stage, but logs for information, such as successful logins, account activity and data access, provide key data at subsequent attack stages.

However, increasing monitoring can generate a tremendous number of logs, and discovering actionable intelligence from manual review is a significant challenge. To ease that burden, your organization can implement a security information and event management (SIEM) platform to automate log collection, aggregate logs and provide intelligence analysis. SIEM consolidates logs from a vast array of devices into one place, normalizes data to a common taxonomy and generates new alerts based on unique criteria.

Corrective controls

Corrective controls are designed to limit the scope of an incident and mitigate unauthorized activity. These measures provide support for post-incident activities and help you understand how to improve your preventive and corrective controls moving forward. Many organizations view corrective controls as technical, but they can also be physical, procedural and legal or regulatory in nature.

Organizations often focus corrective controls during a full breach, but they should be implemented earlier to reduce your risk of harm. For example, during the infiltration stage, you can identify and block attackers during the initial exploitation. Hackers can be deterred from gaining the full access they need to progress to later stages and cause more damage.

The propagation stage is the most critical time to implement corrective controls. Organizations often miss critical opportunities to identify true issues, rather than just symptoms. When properly implemented, the early information collection and analysis can keep an event from becoming a more serious incident.

The aggregation stage is where the issue transitions from an event to an incident. Corrective actions are focused on breaking access to data at the source or staging point and disabling the hacker's ability to remove information from your environment. Typical methods include disabling offending accounts, resetting passwords and blocking or isolating offending IP addresses.

As mentioned earlier, the exfiltration stage is the primary focus of corrective controls in many organizations. Compromised data, such as intellectual property, cardholder data or financial information is the objective, as incident response teams tend to focus on repairing the issue, rather than preserving evidence. This is not necessarily the wrong approach, but balance is often needed earlier in the process.

Organizations can implement several initiatives to mitigate costs and risks. From an administrative perspective, companies can develop a written information security program (WISP), vendor management protocols and business continuity and disaster recovery plans. Specific preparation tasks include performing an information technology (IT) risk assessment and implementing an incident response plan, mock incident response drills and security awareness training. Incident response documentation is also valuable, including how an incident was discovered, what actions were performed, when the event occurred and the ultimate results.

Several technical tasks can help correct any potential issues, including implementing a data classification and integration program. Organizations can also benefit from network and application patch management, as well as backup and archiving solutions and network vulnerability testing. Enterprise monitoring solutions can provide event logging and enhanced data loss prevention capabilities.

There are no silver bullets to protect against incidents and there is no one-size-fits-all approach to developing and implementing security controls. The reality is that you likely will suffer a breach, but implementing the right preventive, detective and corrective controls makes your organization more difficult for hackers to exploit and limit the potential damage.

+1 800 274 3978
www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood®* is a registered trademark of RSM US LLP.

© 2015 RSM US LLP. All Rights Reserved.