Protecting Your Mid-Size Business from Today’s Security Threats

In this issue:

Think You’re Too Small to Get Hacked? Think Again

Security and Compliance: Similar but not the same

How Do You Know When You Need More Security?
Contents...

Contributor: Michael Pastore

Protecting Your Mid-Size Business from Today’s Security Threats

2  Think You’re Too Small to Get Hacked? Think Again

5  Security and Compliance: Similar but not the same

8  How Do You Know When You Need More Security?
Think You’re Too Small to Get Hacked? Think Again

By Michael Pastore

If you were one of millions of customers who used a credit or debit card at Target between Thanksgiving and Dec. 19, 2013, you’re well aware that your card number and even your PIN are likely for sale on some dark corner of the Internet. The incident garnered extensive media coverage because of the size of the breach, the timing, and the fact that hackers managed to gain access to Target’s point-of-sale system itself and steal sensitive data.

As a victim, you also got a flurry of emails from your bank outlining protective measures, precautions, and were more than likely informed your account was being cancelled and a new card was headed your way. Even if you failed to shop at Target during the 2013 holiday season you’re certainly aware of the breach.

Target wasn’t the first major retailer to be hacked. In 2007 TJX Co., the parent company of T.J. Maxx and other retailers was the victim of a breach that pilfered approximately 45 million debit and credit card numbers.

Incidents like these make headlines because of the amount of damage they do — to the customers, to the brand, to the employees, and to the shareholders. Think of it this way: when someone has their wallet stolen it rarely makes the news; when millions of people wake up one day and their wallets are gone, that’s a story.

Breaches at big brands make the headlines, but mid-sized businesses are also vulnerable to cybercriminals. In fact, midsize businesses are a more appealing target for some hackers because they often lack the security expertise to prevent and detect attacks, which means once the bad guys gain access, the breach may go undetected for a long time.

Some hackers are undoubtedly motivated by making headlines and look for opportunities to pull off very public attacks like the Target breach. But for others, hacking is a crime of opportunity. They look for the path of least resistance and make their move. Just because your business isn’t a multibillion dollar corporation with a well-known brand doesn’t mean your data is worthless. Data is data. It all has value.

How common a problem are data breaches among small and mid-sized businesses? A 2013 study by The Ponemon Institute found that 55 percent of small and mid-sized businesses had experienced a data breach, and half of those businesses experienced multiple data breaches. In some ways the stakes are higher for SMBs. TJX and Target took a hit to their brand and their stock price, but they will certainly recover. According to the National Cyber Security Alliance, 60 percent of small businesses will fail within six months of falling victim to a cyber attack.
Has Your Business Been Hacked?

Hackers don’t openly advertise their presence once they gain access to your systems, and if your mid-sized business lacks security expertise or the right tools, a data breach can go undetected. Even a breach on the scale of the Target incident went unnoticed for the better part of a month. The chances are good that if your business is hacked it won’t be you who notices it. According to the Verizon Data Breach Report 2013, 69 percent of data breaches were reported by an external party, with 9 percent reported by customers.

Much like the human body, the health of your business is a constant struggle between methods of infection and protection against illness. That makes information security vital to your business’s survival.

Criminals use a number of tactics to gain access to your data. Among the most common tactics are:

**Password cracking:** Hackers can use a number of software-based tools to recover passwords stored or transmitted on computers. Brute-force attacks try repeatedly guessing passwords until the right one is found. Dictionary attacks try thousands of words in a short amount of time, which is why so many experts recommend using special characters and punctuation marks in passwords. The bad news is that faster processors make the process of cracking passwords faster and less expensive than it was just a few years ago.

**Social engineering:** Social engineering can be used online and offline to build trust, and many people use that trust to gather information such as passwords or physical access to a secure area. Today’s online social networks mean many people are sharing information with people they don’t know well and may not have met in person. Simply put: the same con games that used to take place offline are now taking place on the Internet.

**Packet sniffers:** Also known as packet analyzers or network analyzers, packet sniffers can intercept network traffic on both wired and wireless networks. There are a number of legitimate reasons for network experts to use packet sniffers, but they can also be used to spy on network users. These tools are a major reason mobile users need to be careful about where they log on to networks outside of their organization.

**Vulnerability scanners:** Vulnerability scanners are used by remote attackers to look for areas of weakness in a computer network. Once a known vulnerability is found (e.g., a patch was not applied to a software application) the attackers can exploit that vulnerability to gain access.

**Phishing:** A phishing attack is a type of social engineering attack that attempts to use email or social media to get information from a user. A phishing attack might involve an email that appears to be from a bank representative or the IT help desk and direct the target to a fake website where sensitive information is willingly surrendered.

**Viruses:** For many users, viruses were their first introduction to computer security. Early viruses were spread by physical media like floppy disks, email files, infected websites, and chat applications. Many early viruses were nuisances written by bored programmers, but today international crime syndicates and national intelligence agencies employ viruses to gain access to intended targets.

“Hackers don’t openly advertise their presence once they gain access to your systems, and if your mid-sized business lacks security expertise or the right tools, a data breach can go undetected.”
While bad guys have their methods for conducting attacks, your business needs to utilize different methods to keep its information safe and secure. There are, of course, a number of technologies that should be deployed to increase security, including firewalls, antivirus, and security information and event management (SIEM) solutions. For remote access, virtual private networks (VPNs) should be employed. There is also education that should be disseminated to users, such as published security policies that govern how and where devices can be used and secured, as well as enforced regulations governing passwords. In the end, passive security is not enough.

Even if your business has the personnel with security expertise, the process of information security is never complete. Employees come and go and processes change, and through it all you need to maintain security. Many mid-sized businesses are challenged by their reliance on point solutions that each provide a piece of the security puzzle. Unfortunately, they are not designed to work together, and over time many of these solutions compounded the complexity without a holistic view of the organization’s security program.

Recurring security assessments, which can be conducted annually by a third party, will let your organization know where its security practices stand in relation to other businesses and in relation to the risks of the evolving, ever-changing security landscape.

HP Enterprise Security Products (ESP) Global Services conducts a Security Operations Maturity Model (SOMM) assessment that focuses on the key areas of people, process, and technology. It uses interviews, documentation reviews, discussions, and observations to create a report outlining the results, key findings, and recommendations.

HP ESP consultants can also conduct a Security Operations Primer, which can help your business set up its security operations center (SOC) leveraging established best practices developed by professionals who have seen the best and worst of information security.

HP ESP also offers a number of software solutions to help improve security. Its HP ArcSight Security Intelligence platform is a SIEM solution that helps businesses gather and correlate security and non-security related information to provide a broad view of activities that may be indicators of a security breach. HP ArcSight is also available in an appliance offering, ArcSight Express, which brings enterprise-class defenses to mid-sized businesses.

Conclusion

Despite the attention given to data breaches at major brands, mid-sized businesses are just as vulnerable, if not more so. These organizations often lack security expertise on both the technology and process level.

Mid-sized businesses need more than a basic understanding of the common tactics used by hackers and the technologies they can deploy to defeat them. They need to make security a continuous process with the help of annual assessments and the establishment of a security operations center. HP Enterprise Security consultants can help provide the technology, processes and people that make security a top priority for mid-sized businesses.

Keep reading this eBook for more details on HP ESP security assessments and the HP ArcSight SIEM platform.
When a large security breach captures the attention of the general public, the topic of information security quickly comes under a lot of scrutiny. The media coverage and statements by politicians are nothing new, but these incidents often remind businesses that there’s no time like the present to review the steps they are taking to secure their IT infrastructure.

Among the steps businesses might include with their security practices are those they are using to remain in compliance with industry or government regulations. In the minds of many mid-sized businesses, security and compliance go hand-in-hand. The truth is security and compliance are inter-related, but they aren’t the same thing.

Both security and compliance protect the business from risk. Both security and compliance are used to reduce the chances that bad things will happen to the business, whether it’s protecting data from malicious outsiders or tracking which employees have access to which data internally. Both security and compliance provide visibility into the IT infrastructure, which is always a good thing. They can help businesses determine what’s protected, what needs more protection, and detect changes in the environment. If either security or compliance is ignored there’s a price to pay, in fines, lost business, and a soiled reputation. That’s where the similarities end, however.

One of the main differences between security and compliance is that the requirements to be in compliance with regulations are usually pretty well defined. Businesses can make a list of the conditions they need to meet, then deploy the software and establish the practices they need and check off the boxes. Security doesn’t work the same way. Security needs to constantly evolve to keep up with the latest threats, and industry organizations and government bodies that mandate compliance simply don’t work that fast.

For a number of years early in the 21st century, as regulations like Sarbanes-Oxley were established following a number of well-publicized accounting scandals, compliance actually drove investments in security. Under threat of severe penalties, businesses went to great lengths to ensure their data was secure and access to IT assets was properly limited. But those great lengths usually went only far enough to meet the
compliance regulations — and being in compliance falls short of being secure. Need proof? It’s a safe bet that Target, a publicly traded enterprise with an army of IT professionals, experts in corporate compliance, and a market cap around $40 billion, was certain it was meeting its compliance obligations when its data breach took place during the 2013 holiday season.

Many mid-sized businesses that need to meet compliance regulations are handling compliance in a similar manner to the way they manage security. They are doing what needs to be done and deploying the software tools, but they likely don’t have a lot of in-house expertise on the subject. Among the point solutions they are deploying is log management software that monitors the comings and goings that take place on their IT infrastructure, and they more than likely see such solutions as providing both security and compliance benefits.

SIEM Solutions for Security and Compliance

Log management tools are good at aggregating data from servers, applications, databases, and networks but where they fall short is extracting any real meaning from the data.

If, for example, a change to a server configuration forced a business-critical application to fail, an analyst could use log management software to see who logged into the server and made the change. It’s easier than sifting through the raw log files from the server, but on the other hand, the damage is already done. The analyst is only looking because the business already suffered costly downtime.

The concept of log management has evolved in the past decade into security information management (SIM), security event management (SEM), and now security information and event management (SIEM). More than just collecting and passing on log files, SIEM solutions gather the data, examine the data for correlations, and pass the data along in usable forms, such as alerts in the case of an emergency or dashboards that display the data in an easy-to-use format.

Sticking with the example of a server configuration change that causes application downtime, a good SIEM system would see the danger in that change in real-time and send an alert to an administrator.

SIEM systems also retain the data so events that happen today can be correlated to events that happened in the past. Data retention also helps with forensic analysis of the data.

Like all forms of data that businesses are dealing with today, the data that is collected by SIEM programs from devices, applications, databases, servers, and more is growing exponentially. There’s too much data to allow for timely analysis by human security analysts, which means by the time something out of the ordinary is mined from this big data it’s going to be too late.

In the recent past many mid-sized businesses would consider investing in a full-fledged SIEM application to be overkill. But with the amount of data that needs to be collected and correlated, and the high stakes of not having visibility into the infrastructure, SIEM solutions are worth exploring, especially for mid-sized businesses that lack a high degree of security expertise.

The HP ArcSight Security Intelligence platform is a SIEM solution that collects, analyzes, and assesses IT

“Many mid-sized businesses that need to meet compliance regulations are handling compliance in a similar manner to the way they manage security.”
security, business security, and non-security events in real-time. It then rapidly identifies, prioritizes, and passes the information along for an appropriate response. HP ArcSight can correlate billions of events each day to find threats and vulnerabilities that can negatively impact the business.

HP ArcSight users get complete visibility into their IT infrastructure, which helps protect the business from a number of threats to both security and compliance, including:

- Malware
- Hackers
- Internal threats
- Corporate fraud
- Application flaws
- Configuration changes

HP designed its HP ArcSight Express offering especially for mid-sized businesses. This SIEM offering provides the same threat protection as the enterprise version of HP ArcSight, but is easier to set up and deploy and is built for the smaller data volumes generated by mid-sized businesses. The rules and correlations used by HP ArcSight Express are identical to those used in the enterprise product. ArcSight Express includes pre-loaded connectors to many popular security vendors, like Cisco and Blue Coat Systems, along with pre-built use cases so users can improve their information security. With HP ArcSight Express, these businesses no longer need to worry about paying for capacity or functionality they don’t need. It provides enterprise-class protection for mid-sized companies.

**Conclusion**

Many mid-sized businesses are subject to compliance regulations imposed by industry or government organizations, and many make the mistake of thinking their compliance practices are keeping their IT infrastructure secure. Security and compliance have a lot in common, but they aren’t the same thing.

SIEM solutions take log management to the next level, collecting and correlating millions of events and passing them on for an appropriate response. As the amount of data generated by businesses continues to grow, SIEM solutions that can sift through big data and identify important events and make correlations are essential to providing a secure IT environment. HP ArcSight is an industry-leading SIEM platform that can collect, store, and analyze big data. HP ArcSight Express delivers the same functionality in an easy-to-configure package designed especially for mid-sized businesses.

Using HP ArcSight solutions can help businesses maintain compliance with industry or government mandates and are an important part of creating a secure IT environment. Best-in-class security still requires further investments in technology and manpower. Visit www.hp.com/go/arcsight to learn more.
There is a saying in the medical profession, “prevention is the best treatment.” The same can be said for information security. Waiting until your business has suffered a security breach is too late to realize you need security. The truth is your business always needs security. As it grows from a truly small business into a mid-sized business, there are a number of established best practices it can follow. When it comes to network security, IT professionals can search for holes in the firewall that hackers can exploit. It can also provide secure access to remote employees using a virtual private network (VPN) to keep applications and data secure regardless of the user’s location. Other established approaches include the deployment of endpoint security products and strong password policies.

These established approaches to security are mostly well known by now, but they pose a couple of problems for mid-sized businesses. The first is that many mid-sized organizations lack the skills, resources, and expertise to properly deploy and maintain the technological side of IT security. Security responsibilities at mid-sized businesses often fall to IT generalists who are also tasked with managing servers and other applications.

The second problem established approaches to security pose for mid-sized organizations is that they are too reactionary. Even if steps are taken to implement security before there’s a breach, the threat landscape is constantly evolving. In an organization with limited resources and IT security expertise, the chances are good that the bad guys will find a problem with the defenses before the good guys will.

Mid-sized organizations can overcome these issues by seeking help from outside security experts. Security, after all, is best viewed by a trusted party from outside the organization that is looking for a way to get in. Managed security partners, simply put, are good guys that think like the bad guys.

Third-Party Security Assessments

A third-party security assessment gives businesses a holistic look at their technology, policies, and practices around information security. This is especially helpful for mid-sized businesses that are deploying point solutions to tackle different areas of their IT security and lack dedicated IT security professionals.

A comprehensive third-party security assessment includes overviews of the technology, but also examines the culture around IT security. A third-party assessment will use interviews with stakeholders to learn how security practices are standardized and, for example, what
happens to those practices when an employee leaves the organization. It can also uncover the attitude of corporate executives toward IT security, which can range from viewing security as a risk manager and business enabler to seeing it as a cost center that consumes budget but adds little to the bottom line.

After an assessment, the managed security partner will have recommendations that discuss ways to improve the organization’s security from every angle — technology, people, and practices. But it’s also important that it doesn’t end there. Experts recommend an annual assessment that can track the progress of the organization’s IT security practices and compare them to the constantly evolving threat landscape.

HP Enterprise Security Products (ESP) Global Services conducts assessments that gauge the maturity level of a business’s security operations. This assessment helps organizations determine where their security maturity stands in relation to other organizations in the industry and the greater threat landscape. The assessment usually takes three days, and assesses the technology, includes interviews with stakeholders and security and analysts, and examines the organization’s security processes to see, for example, if they are standardized.

After the assessment the organization is rated according to HP’s Security Operations Maturity Model (SOMM).

The objective of the HP ESP Global Services assessment is not only to determine the maturity of the security operations, but also to provide tactical recommendations the business can use to improve the maturity of those operations. The recommendations cover technology, people, and processes and help the business align with information security best practices. A roadmap is then developed to help the business achieve significant improvements in its security capability using distinct phases, starting at the current level of monitoring and evolving through two phases to a single mature security operations capability. It’s recommended that the HP SOMM assessment be conducted on an annual basis.

Conclusion

Mid-sized businesses need to establish effective IT security as they grow, but many are lacking the resources and expertise needed to deploy and maintain the technologies, practices, and policies that make this possible. Third-party security assessments from a managed security partner can help businesses get a holistic view of their IT security, bringing together information about various point solutions and understanding how IT security is viewed as part of the business as a whole.

HP ESP Global Services conducts assessments that measure organizations’ security maturity using HP’s Security Operations Maturity Model. Each assessment is followed up by recommendations and a roadmap, which helps organizations improve their security operations and reach a level of continuous improvement that helps keep pace with the evolving threat landscape.

<table>
<thead>
<tr>
<th>SOMM Level</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0</td>
<td>Incomplete</td>
<td>Operational elements do not exist</td>
</tr>
<tr>
<td>Level 1</td>
<td>Performed</td>
<td>Minimum compliance requirements to provide security monitoring are met</td>
</tr>
<tr>
<td>Level 2</td>
<td>Managed</td>
<td>Business goals are met and operational tasks are repeatable</td>
</tr>
<tr>
<td>Level 3</td>
<td>Defined</td>
<td>Well-defined, subjectively evaluated, and flexible operations</td>
</tr>
<tr>
<td>Level 4</td>
<td>Measured</td>
<td>Operations are quantitatively evaluated, consistently reviewed, and proactively improved</td>
</tr>
<tr>
<td>Level 5</td>
<td>Optimizing</td>
<td>Operational improvement program has been implemented to track any deficiencies and ensure all lessons learned continually drive improvement</td>
</tr>
</tbody>
</table>

Security Operations Maturity Model defined.