# Table of Contents

**Introduction** .......................................................... 4

**Chapter 1:**
Data Security: Is Your Data As Secure As You Think? ............. 6

**Chapter 2:**
IT Security Audit: Shifting the Focus from Technology and Tactics to People and Processes ............. 11

**Chapter 3:**
Focus on Four High-Value Controls .................................................. 13

**Chapter 4:**
How to Respond When A Security Breach Occurs .............. 15

**Chapter 5:**
Managed Security Services: Examining the Need for an Outside Firm ........................................ 17

**Conclusion** .................................................................. 21

**About** ........................................................................ 22
Introduction

Too many organizations operate under the false assumption that once they’ve implemented a few cyber security controls, then they’re safe from all potential breaches. It simply isn’t true.

Just ask retail giants Target and Home Depot. Their security strategy featured many technological bells and whistles. In the case of Target, it was a gap in third party vendor security that gave hackers the loophole they needed to infiltrate their system and steal reams of customer data.

They’re not alone. Despite their best efforts, many organizations’ programs and tools are not as effective in mitigating breaches as they’d like to believe. A 2014 Ponemon Institute data breach preparedness study found that 43% of companies surveyed were victims of a breach in the previous year. Disconcertingly, 27% of survey respondents lacked a data breach response plan and/or team. So what can an organization do to make its systems less vulnerable to attack?

Developing a cyber security strategy and implementing processes to manage and monitor the program are key. Without these crucial first steps, buying and deploying more technology products will be for naught. It certainly won’t stem the flow of potential breaches.

If the myriad data breaches over the past 24 months have taught us anything, it’s that we need a different approach and mindset. Security intrusions and data breaches aren’t going away anytime soon. The cyber hackers just continue to find new ways to crack organizations’ security systems.

1. Ponemon Institute’s “Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness” September 2014
The sooner we face the problem in a more effective manner, the faster we will reduce breaches. We need to stop throwing money at the problem and retool how we assess, implement, monitor, test and update our systems.

This guide will provide practical strategies for improving security including:

- Risk assessment tips
- Identifying stumbling blocks that lead to greater security vulnerabilities
- Implementing better processes and controls
- Do’s and don’ts for mitigating cyber crime
- Considering what security tasks can be handled in house and which need the help of an outside firm

We hope you’ll find this guide a good first step in evaluating and improving your cyber security program.
Chapter 1

Data Security: Is Your Data As Secure As You Think?

When the topic of reviewing an organization’s security program is raised we often hear any number of the following responses:

- “We just invested in security technology upgrades.”
- “We trust that our vendors have adequate security.”
- “Our data wouldn’t be of value to anyone outside of the organization.”
- “Our organization implemented a security program a few years ago and we haven’t had any problems to date.”
- “We’re PCI-compliant, so we don’t have to worry about a breach.”
- “Our people are trained well enough.”
- “We’ve got that covered.”

Unfortunately, there is a fault in the logic behind each response.
Chapter 1

Technology Is Not a Panacea

Many organizations mistakenly believe that purchasing network security technologies translates to “one and done”. That belief makes them a prime target for security breaches. Thinking “We’ve already got security technology tools in place, so we don’t have to do anything else” is precisely what cyber criminals bank on — complacency and a false sense of security.

What’s more, even if your organization regularly invests in and implements security technology upgrades, those alone are not enough to deflect all security breaches. Take for example the case of Target. All the upgrades in the world could not have prevented the breach they suffered. In that case, an outside vendor used to conduct routine maintenance on Target’s refrigeration systems became the breach entry point when his vendor credential information was stolen. This case illustrates why technology alone is not a panacea.

Vendor Security Up to Snuff?

In that same vein, don’t assume that your vendors have adequate security measures in place. As was the case with Target, the U.S. Office of Personnel Management (OPM) became vulnerable in part through KeyPoint, one of their vendors. KeyPoint, a background check vendor for U.S. government security clearances, had previously suffered a breach attributed to China by many reputable sources.

Various sources have reported that user credentials compromised during the KeyPoint breach were used to facilitate the highly publicized OPM breach, which was also attributed to the Chinese government. The lesson learned for organizations — is do not assume that your preferred vendors are immune to attacks, or that they even have an effective security program in place.

Identifying Targets Using Data Value Analysis

According to a June 2015 SecurityWeek article, “Many Organizations Lack Maturity to Address Security Risks”, nearly 75% of organizations worldwide

are not equipped to address cyber security issues. Even if your organization is one step ahead of most on the cyber security curve, are you properly assessing the value of your data? Don’t assume that your organization has nothing of value to steal or that you’re too small, and therefore, able to fly under the radar of cyber criminals.

It’s not just credit card, bank or social security numbers that hackers are after. Intellectual property and personnel information are other types of data that can be used for malicious intent or can be sold on the black market. OPM can attest to it. When their system was hacked, it exposed sensitive information for up to 22 million former and current federal employees as well as applicants, spouses and partners. Worse, it compromised highly sensitive security clearance information — highlighting the ripple effect of such breaches and striking a significant blow to our national security.

**Cyber Security Is a Marathon, Not a Sprint**

Large or small, just because your organization has managed to operate in a hack-free environment, you shouldn’t be complacent. When it comes to security, you can’t live by the adage, “No news is good news”. Cyber criminals are always scheming and devising new ways to break into systems. And if the cyber criminals are continuously working to hack systems, then you should be monitoring and testing your networks and systems just as vigilantly.

Look at cyber security as a marathon. You have to lay the groundwork for a successful marathon by creating a training plan — your security program. Then you need to consistently and diligently train for the marathon by running through security procedures and monitoring the system. Next you must run through the possible scenarios of marathon day and figure out how you’d handle them. Like a marathon, robust network security is a long and arduous process. Proper planning, training and testing will go a long way to ensuring you maintain an effective security program.

**Compliance Does Not Equal Security**

Many organizations find the task of implementing HIPAA or PCI compliance requirements, daunting and time-consuming. Because compliance regulations are constantly changing, it is also difficult for many to keep up-to-date. Others find it challenging to identify and heed the compliance requirements relevant to their specific organization’s needs, and data protection requirements.
At the same time, it is not a good idea to rely too heavily on compliance as the cure-all for your security needs. Don’t become “compliance complacent”. A strong security program cannot be placed into a compliance checklist, but needs to come from balancing risk and business impacts with controls.

Assessing Your First Line of Defense — Security Training
With many organizations, training is insufficient, incomplete or worse, non-existent. Naturally, cyber criminals realize this weakness and use it to their advantage. Don’t assume your employees can figure it out on their own or that a proper training program isn’t worth the investment.

According to the 2015 Cost of Data Breach Survey from the Poneman Institute it costs an organization an average of $145 for each customer record breached. Multiply that across your customer base and that can add up to a costly line item.

Every organization should train their employees to detect security red flags — including common phishing techniques. Employees need to be trained in how to spot phishing tactics as well as how to report them quickly so they can be contained should an attack slip through the controls.

Maintaining a Security Program Requires a Specific Skillset
Not everyone has an in-house cyber security expert with the right background to identify issues and to implement and manage a security program internally. This requires a very specialized skillset. It’s why outsourcing is often a good option to consider. What’s more, you can designate precisely which areas of security you’d like an outside security vendor to handle, from risk assessment consulting to around the clock monitoring.

Many organizations use third-party cyber security providers to look for patterns (and malware) across their client networks. Others opt for using security consultants to develop strategies to avert attacks and for ongoing
testing of controls. If breached, they use them to help contain the problem, restore normal business operations, and ensure that all areas of the network are secure again, not just the area that was identified in the breach.

**Adopt a Proactive Stance**

The key here is to be proactive about security. Become knowledgeable. Join a local chapter of the Information Systems Security Association (ISSA) or InfraGaurd, a public/private partnership between industry, academia, law enforcement agencies and the FBI. Get educated, and you’ll learn incrementally over time how to improve your organization’s cyber security management.

In the next chapter we’ll look at why security teams should focus on people and processes, not technology and tactics when conducting risk assessment of security programs.
Initially focusing on technology tools is akin to putting the cart before the horse. Instead, a thorough assessment of risks and a plan to manage them are more appropriate first steps for improving security.

**Shift Your Focus**

There needs to be an intrinsic shift in the way organizations address and reduce security breaches. That shift begins with reviewing and assessing an organization’s processes and people.

Below is the path we recommend for mitigating security risks in a more holistic fashion. Each step is in listed in of order importance and implementation. All work synergistically to strengthen an organization’s network security, and reduce their exposure to potential breaches.

1. **Risk Assessment:** Several methodologies are available, but they all break down to the same basic tasks; inventory your information assets, examine vulnerabilities, analyze potential threats and evaluate the resulting risk. This is a critical piece
of your security program, so take time to get it right. If you need help, find a qualified external professional to assist.

2. **Processes:** Develop and deploy processes to run and monitor your security program. This piece is often skipped but it’s the “make or break” step for a successful security function. Ideally, processes should be developed before you purchase new technology.

3. **People:** Assess security knowledge and readiness of staff. Determine security chain of command and protocols. Institute and deploy a detailed security training program. If necessary, bring in an outside firm to provide staff augmentation or business process outsourcing for areas where you don’t have adequate skillset on staff.

4. **Technology:** Analyze present technology, then determine and implement any necessary upgrades. Get personnel up to speed with procedures and controls through training. Routinely and consistently monitor, test and patch.

Continue to Chapter 3 to learn how better controls and processes can reduce your risk of a data breach.
Chapter 1

Network Security Best Practices for Prevention, Detection, and Response

Chapter 1

If implemented properly, the following four controls can greatly improve the security posture of most organizations:

1. **Use network segmentation and network access controls to protect sensitive data.** Though it may be more convenient for internal stakeholders to interconnect all of your digital functions, doing so can leave your organization more vulnerable to breaches. Instead, identify systems which process and store your sensitive information, segment them onto different networks, and implement network access controls to protect them.

2. **Employ application whitelisting.** As opposed to blacklisting, where you prohibit specific functions, applications or users, whitelisting green lights or approves access only to certain applications, users and functions. This move greatly reduces the opportunity for a non-approved user or application to infiltrate the system.

3. **Review your patching/vulnerability management program.** Installing security patches to fix flaws in software has become a routine task for IT teams across the globe. And given the myriad of
applications used by organizations today, it’s important to have a means of validating that all the required patches have been applied. That’s where a vulnerability management program can help. Vulnerability management tools scan your systems looking for missing patches or updates — just like an attacker would. The reports they generate let you know if you’ve missed anything, and tell you where to focus your patching efforts.

4. An intrusion detection capability — both network traffic and log monitoring. Cyber criminals bank on organizations being complacent with their intrusion detection monitoring. Both servers and network infrastructure should be regularly monitored for unauthorized incoming connection attempts, incoming port scans, unusual root or administrator access activity, and modification of file systems. If we can agree that it’s impossible to prevent 100% of attacks, then it’s absolutely necessary to have a good detection capability so we can know when an attack succeeds. This early detection allows your organization to contain the impact and return to normal operations quickly.

Now, let’s explore more ways to further reduce security breaches as well as effective containment and communication strategies in the aftermath of a breach.

This early detection allows your organization to contain the impact and return to normal operations quickly.
Chapter 4: How to Respond When A Security Breach Occurs

Now that we’ve covered the path to mitigating security risks through risk assessment, processes, and people, we need to identify what will be done if a data breach does occur.

This problem isn’t going away in the foreseeable future. And just because you haven’t identified an intrusion or other data loss event doesn’t mean you haven’t had one or won’t ever have one — even if you are “doing everything right”.

Preparation is a vital component to mitigating cyber threats. As the saying goes, “Fail to prepare, prepare to fail.” Be proactive and plan ahead, and make provisions for as many potential cyber security breach scenarios as possible and make sure you have a documented Incident Response Plan that covers them. If you’re starting from scratch, The National Institute for Standards and Technology Special Publication 800-61 (NIST SP 800-61) provides detailed instructions on building an incident response capability, including a handy incident response checklist.

With that in mind, we recommend you employ these strategies to respond to security breaches:

• Containment: Don’t delay your response once an intrusion is identified. Do carry out your containment procedures with expediency. Containment strategies will vary, depending on the nature of the attack. In some cases it will be appropriate to shut down affected systems quickly. In others, you will want to keep them up and closely monitor the attacker’s activities in order to gain additional detail that will be helpful during the remainder of the
response. Having a comprehensive Incident Response Plan to guide your actions can be the difference between success and failure.

- **Eradication & Recovery:** Once the incident is contained, it’s time to start cleaning up the mess. Do rely on your Incident Response Plan to guide Eradication & Recovery efforts. During eradication, you will identify all affected systems and perform activities appropriate to the incident type, such as removing malware or changing passwords on breached user accounts. Recovery activities typically involve actions like restoring files from backup, or installing missing security patches. These efforts are intended to get you back to normal business operations.

- **Communication:** Notification of internal and external players: Don’t delay in communicating with internal departments and external vendors, partners and clients. Do outline a clear chain of communication before breach detection and follow it post-breach. Depending on your industry and state, laws vary with regard to required deadlines to inform those affected by the breach.

Following proper procedures carefully and quickly can minimize breach fallout. Remember:

- Contain the breach
- Assemble the response team
- Investigate the breach
- Document the who, what, where, when, why and how of the breach as well as the relevant notification time limits
- Inform authorities and insurance companies
- Follow your breach communication procedures

Next, we’ll consider the questions you need to ask yourself to determine if you should work with an outside security consulting firm.
The Wisdom of Collaboration

Surprisingly, less than half of the Ponemon Institute’s 2013 respondents had a plan for responding to breach attacks. On the other hand, 82% of companies with highly effective security practices collaborated with other technology experts, such as the Information Sharing and Analysis Centers forums (ISACs), to better understand and deal with security and threat trends.

More secure organizations recognize that no man, or in this case, no organization, is an island. Collaborating with other organizations, partners, vendors, and agencies to mitigate cyber threats and reinforce network security programs is a smart approach.

For many organizations, working collectively to reduce cyber threats leads to the question of whether they are inclined and/or capable of assessing, developing, implementing and managing their network security program in house or whether, farming out all or some of these tasks to a managed security services provider (MSSP) is a better fit.
In-House or Out-Source?
So how do you know if your organization is equipped to tackle a network security program on its own? When is it best to look to an outside security firm for guidance? Below, we help you weigh each option.

Answer the following questions to help gauge how well your organization can address them and which areas are best left to outside vendors:

1. **Do you have the manpower to oversee a robust network security program?** Such a program requires 24/7 monitoring and response, (intrusion containment, patching, etc.). If you’re a small to medium sized business or start up, employing a dedicated person or team might be beyond your scope or budget. What’s more, tackling it on your own could shift the focus to the minutiae of monitoring and trying to keep pace with security threats and away from your core business.

2. **Do you have a comprehensive security program in place, and hired a team that possesses adequate knowledge and expertise in planning, implementation and management of network security programs?** As a whole, these steps can be daunting, even for those who know where to start and how to start. For many organizations, keeping up with compliance issues and new regulations can become a job in and of itself.

   Then there’s the ongoing challenge of finding qualified people. For the moment, there aren’t enough security professionals to fill the available positions in the market. This shortage has put a premium on salaries for skilled security professionals, often putting them out of reach for smaller organizations. Some companies have turned to managed security services providers to provide resources in the face of this talent shortage.

3. **Does your IT team possess the highly specialized knowledge needed to handle high-maintenance security technologies, such as Security Information Event Management (SIEM)?** As we’ve mentioned earlier, many organizations today tend to purchase security technology products and deploy them in a “fire and forget” manner. They expect the tools to function effectively with
very little effort from their staff. As we’ve seen with the recent spate of security breaches, this simply does not work, especially for complex systems like SIEM platforms.

SIEMs are wonderful tools, and with a knowledgeable security analyst at the helm, they can provide insight into security events that would otherwise go unnoticed. However, they require a great deal of routine care and feeding to operate effectively. Because most companies don’t want to dedicate a full time resource to SIEM administration, these expensive systems will often be neglected and the expected return on investment will never be realized.

This is a perfect area to seek help from outside professionals, such as Managed Security Service Provider or MSSPs. The MSSP can provide resources to administer the technology and then deliver the output to your team for action. This type of relationship allows your internal team to focus on running your business and delegates the more mundane and labor-intensive activities to a service provider.

4. Does your organization understand how to ensure that your risk assessment also covers critical compliance issues with multiple frameworks and standards including NIST, HIPPA, PCI and more? Risk Analysis and Risk Management are complex activities that front-line IT staff often struggle with. If your team does not have experience performing them, an outside consultant can often save you time and money by providing a process that encompasses all of your business operations and compliance requirements in a single risk management framework. Most importantly, these are two activities that drive the rest of your information security efforts — so — it’s critical to get them right.

5. What is the cost benefit analysis of in house network security versus outsourcing? Your initial assumption might be that you can save money by handling it yourself; or that all outside consultants will be cost prohibitive. We recommend you analyze costs and speak with several vendors. You may discover that it is more appropriate and cost-effective to outsource. And if your organization is not experienced in network security, then you should absolutely look for a reputable outside firm to handle your security for you. Perhaps you have the manpower and expertise for some but
not all security tasks. Many security providers are flexible and open to a customized, a la carte approach — perhaps just handling one or two areas for you.

You may not necessarily need an outside firm to provide a full turnkey solution. However, if you’re not sure where to begin but are committed to “getting it right the first time”, a consultation with outside security firm is a good starting point. A thorough risk assessment, with actionable implementation steps, is well worth the associated fee, if it means you save your organization from costly breaches later.
**Conclusion:**

Even the most diligent companies can fall short on keeping their security up-to-date and effective in mitigating breach risks. As previously noted, breaches aren’t going away. Throwing money and technology at the problem isn’t an effective approach.

Cyber criminals are committed to staying one step ahead of everyone else. Don’t let them fly under the radar. Be proactive and eliminate any issues or trouble spots that grant cyber criminals easy access.

Don’t be discouraged by the magnitude of the task. Keep in mind Plato’s maxim, “The beginning is the most important part of the work”.

The first step is moving from a knee-jerk, technology-focused response to a proactive, holistic one. Next is risk assessment, then developing, implementing and managing your network security program. Some organizations can handle it completely on their own…but not very many.

Most organizations leave many of these tasks, if not all, to outside experts, especially if they lack the proper staffing and processes to do it in-house. Just as many, after doing a cost analysis, recognize that in the long run, outsourcing some of these tasks can save money and time — providing a definite return on investment.

The potential damage that breaches can cause an organization necessitate that IT teams change their current mindset — moving from a concentration on technology and tactics to an emphasis on strategy and process. There’s too much at stake — not just hard costs, but your reputation, your customers’ trust, and your organization’s valuable proprietary information.

Shift the focus from a cost and investment model of meeting the bare minimum to one that rises to the occasion by tackling the complex, time-consuming issues in a high-performance way. Commit to the strategy and process …and a more effective security program will follow.
LBMC Information Security

While regulatory compliance is mandatory, so is operating a successful business. A well-designed information security program provides critical intelligence about risks facing your business so your executive team can make well-informed decisions.

As a member of the family of LBMC companies, LBMC Information Security separates itself from traditional information security firms by offering practical, cost-effective solutions that are customized to your unique risk environment. We tailor our assessments and deliverables to your organization’s risk tolerance, providing the highest level of risk reduction for the associated cost. These practical solutions lead to real results and a tangible return on investment.

Managed Security Services
Managed security solutions provides around-the-clock monitoring for information networks. LBMC’s 24×7 state-of-the-art intrusion prevention and detection services and Security Information and Event Management (SIEM) solution will keep organizations’ proprietary data secure from unauthorized access. Monitored 24 x7 by cyber security professionals, LBMC’s Managed Security Services are part of an aggressive detection plan that help keep networks safe from intrusion, corruption and data theft.

Ready to discuss your network security concerns?

Contact us for a free consultation:
www.lbmcinformationsecurity.com/contact-us