Introduction

Information security has become a critical business function.

Today’s organizations cannot afford to overlook the security of the mass amounts of data used in daily operations, the systems which store and transmit that data, or the people who rely on that data to perform regular job responsibilities. One look at the constant news cycle illustrates just how vulnerable companies are to the whims of cyber attackers.

Don’t be fooled: It’s not just small businesses with limited resources that routinely fall victim to cybercriminals. Major organizations have grabbed headlines for recent breaches. From the FBI to the IRS, Equifax to Verizon, the list of companies reporting data breaches grows every year because organizations are failing to focus on the security basics which set the foundation for a holistic security program.

Ponemon Institute data breach studies have found that:

- 43% of companies surveyed experienced a data breach.¹

  But only a mere...

- 27% of respondents said they are confident in their ability to minimize the financial and reputational consequences of a material data breach.²

For more information, visit LBMCInformationSecurity.com or call 1 (844) 526-2732
Until enterprises improve detection & response capabilities, attackers will retain the upper hand.

One known vulnerability in commonly-used software or hardware can result in widespread exploitation. The Dyn Distributed Denial of Service (DDoS) attack and WannaCry Ransomware are perfect examples. Criminals understand where companies are likely to fall down in incident preparedness, and they’ll use that knowledge to their advantage.

**Ransomware has become the tactic of choice for financially-motivated threat actors:**

- **50%**
  growth in global Ransomware attacks in the last 12 months

- **$5 Billion**
  in projected damage costs for the next 12 months

- **72%**
  of malware incidents in the healthcare industry involve Ransomware
Ransomware authors aren’t the only ones cashing in on organizations’ insecurity; Nation-states employ highly educated and skilled cyber adversaries who are tasked with exploiting U.S.-based businesses to gain hold of anything that can be sold on the black market or help their foreign entities get ahead. From credit card numbers to financial account information, healthcare records to manufacturing designs and R&D plans, if your company has sensitive or proprietary information, you are a target.

Managing information security is a monumental task, yet most companies don’t have the resources necessary to maintain a fully operational information security program that encompasses:

- People
- Processes
- Technology
- Physical Assets
- Compliance & Regulations
- Oversight of 3rd-party vendors

Companies lacking security expertise are at greater risk of system compromise, potentially costing the organization valuable time, resources, and a hit to brand reputation or bottom line. Developing a thoughtful cybersecurity strategy and implementing processes to manage and monitor the program are key. Without these crucial first steps, buying and deploying more technology will be for naught; it certainly won’t stem the flow of potential incidents.

Security is hard, but you don’t have to tackle it alone. LBMC Information Security can be your partner in (fighting cyber) crime.

**Our comprehensive range of network defense services extends your internal capabilities, allowing you to focus on what you do best while ensuring the information security of your organization’s assets.**

Based on years of experience assisting a large spectrum of companies, the following pages offer our recommendations for evaluating and improving your cybersecurity program.
Prevention

The Issues

Preventing cybersecurity incidents begins with setting a solid foundation.

At a minimum, to keep up with ever increasing security threats, organizations must have the tools to log and monitor network traffic for anomalous or suspicious activity. Traditional intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) systems are costly and often require at least 3 full-time employees to monitor and maintain. As a result, many companies, especially those that are short staffed, end up purchasing expensive tools only to have them turn into shelfware.

It’s not enough to buy the “right tool” for the job; security hardware and software require careful configuration and regular fine-tuning throughout the entire lifecycle to ensure proper security and compliance. If your team is overworked or not sufficiently skilled in continuous monitoring, critical alerts will be missed and not acted upon in a time-appropriate fashion.

Due to news of widespread cybercrime, security software purchases have increased by 40%.

Are these purchases helping companies remain secure?

Of course not—because a tool doesn’t equal security. Security is people, processes, and technology combined, which means that if your organization is missing one of these elements, you’re likely missing important indicators of compromise (IoC).
One of the key ways to harden your systems against security incidents is to ensure they’re up-to-date. As vulnerabilities are discovered—through research or active exploit—vendors roll out patches that can be installed.

Conventional advice says to patch regularly and quickly.

However, in some circumstances this is neither practical nor simple. A vulnerability management program will help you identify and prioritize patch management, and allow you to implement compensating controls for situations when patching needs to be delayed.

Vulnerability management programs help in other ways, too. Just as an attacker would probe your systems for weaknesses, vulnerability management identifies where greater defenses are necessary, highlighting risks to your organization, and providing an opportunity to shore up capabilities.

Companies should perform regular vulnerability assessments and penetration testing.

Organizations often make the mistake of thinking that running an automated scan will do the trick, but your adversaries are using myriad tools and tactics to break into your systems. Your vulnerability management program, therefore, should emulate adversaries’ likely strategies and examine everything from firewall settings and web applications, to how employees and contractors are accessing systems and services, to new application program interfaces (APIs) for third-party developed mobile applications.
Penetration Testing

Hiring skilled penetration testers is one of the best investments your company can make. These experienced professionals are trained to evaluate more than just the technology you use. Pen testers understand the nuances of effective phishing campaigns and will employ real-world social engineering to simulate an attack on your organization and its people. Comprehensive penetration tests are custom designed for your organization and allow you to identify and determine risks in your people, processes, and technology through an understanding of how a threat actor would, in reality, target your organization.

In addition to system and people vulnerabilities, it’s not uncommon for a pen test to surface issues you don’t know you have.

Issues such as uncovering personally identifiable information (PII) or protected health information (PHI) that has been collected by one of the company’s business units then stored insecurely. A reputable firm will not only perform tests and provide a written report with found vulnerabilities, but also offer actionable recommendations for improving your security defenses.

81% of hacking-related breaches leverage stolen and/or weak passwords, and the most common way of obtaining user credentials is through phishing.
Once you understand the weaknesses in your systems, it’s time to develop or update the incident response (IR) plan. Effective IR plans are the playbooks for what actions to take and with whom to work during and after an incident.

**Your IR plan should detail:**

- Who has authority to declare an incident
- Names and contact information of individuals involved in incident handling
- External resources including names and phone numbers
- Organizational roles, responsibilities, and capabilities

And much more. An IR plan that fails to accurately reflect current risks, resources, or capabilities won’t be of much use during the stress and frenzy of a declared incident. As such, it’s not enough to create a plan and stick it in a drawer;

**Organizations need to regularly test the incident response plan and conduct tabletop exercises.**

This will help the organization identify areas for improvement. Acting out a simulated incident response is a great opportunity to learn how your organization might act under pressure and make necessary adjustments before you’re under attack.
Detection

Security event detection is a struggle for most companies.

On average, it takes companies 90-120 days before learning they have a problem.

This means that security teams don’t have a chance to prevent data loss or corruption—the best they can hope for is damage control. This is akin to allowing a thief to enter your home and waiting for him by the front door to stop him from absconding with your valuables. Even with the plethora of security tools available on the commercial market (just like your house surely has more than one door or window), adversaries can circumvent traditional detection methods and inflict harm.

Detecting threats requires a holistic approach that starts with people, prior to a technology purchase. Threat actors rely on unpatched systems, missed or skipped alerts, and known vulnerabilities. Most of the time this isn’t a far-reaching gamble—98% of all exploited systems contained a vulnerability that had been published in the Common Vulnerabilities and Exposures (CVE) database, a tool familiar to all security practitioners, for over one year!

The key to early detection is multi-fold:

1. Secure implementation and configuration of tools (e.g. anti-virus, SIEM, IDS/IPS)
2. 24x7 monitoring for unauthorized incoming connection attempts
3. Incoming port scans
4. Log analysis
5. Unusual root or administrator access activity and modification of file systems
6. External threat intel collection and analysis
7. Alert tracking and remediation
Because of the challenges with detection, many organizations have spun up threat intelligence or threat hunting operations, which help identify emerging cyber threats early in the attack cycle, instead of relying on a passive approach. Threat intelligence requires collecting data from external web sources and combining found information with internal telemetry and data repositories, then aggregating, sorting, and analyzing the whole of information to spot trends and indicators of compromise.

Though this is an overly simplistic explanation, suffice it to say, managing an effective threat intelligence program is complex and requires a specially-skilled workforce.

Threat hunting is gaining popularity because it is a more aggressive method of finding indicators or instances of compromise on internal systems versus waiting for an alert to be triggered, a “bad” IP address to appear in logs, or an employee to contact the help desk with a “situation.” Malware, in particular, needs to be a focus of your detection program, as it spreads quickly and is difficult to contain and eradicate once it has pervaded systems. Using a “converged security” approach to gather and analyze both network and endpoint information, then correlating it with the captured data through threat collection activities, is a new and better process for malware discovery.
Overwhelming?

Partnering with a Managed Security Services Provider (MSSP) can lighten the load of managing your security program, especially if time, budget, or internal staffing is lacking.

In a tight market, acquiring additional staff that possess adequate knowledge of and experience in planning, implementation, and management of security operations and compliance requirements can be daunting and cost prohibitive. Though some organizations worry that working with an MSSP is beyond the company’s financial reach, MSSPs actually provide economies of scale because they already employ trained experts who are working across a wide range of organizations.

As a consequence of their work with various companies across many industry sectors and geographies, MSSPs have a global view of the threat landscape and are current on all the latest attacks. MSSPs provide around-the-clock monitoring (and other services, if desired) so that your security operations never experience downtime.

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.
Preventing and detecting cybersecurity incidents is a massive challenge for which organizations are woefully unprepared, but compounding problems, responding to an incident—or potential incident—is a different ball of wax altogether.

Unfortunately, most organizations aren’t equipped for the inevitable. Responding to an incident requires its own unique set of skills and tools that most companies don’t possess. While certain aspects of incident response are very technical, and expert internal security teams may be able to contain an intrusion or data leak, for instance, incident response is a holistic program that starts well before the company experiences an incident, and stretches well after the threat has been eradicated from your systems.

The common industry term is “incident response”, but what your company should be focused on instead is an incident preparedness plan.

To effectively manage a breach or intrusion, companies need to have a preparedness plan in place that outlines:

- Who is authorized to declare an incident.
- To what external resources the company will need to recruit or call to action.
- How the company will technologically deal with the situation (see page 7).

The incident response plan you (hopefully) built in the “prevent” stage of your cybersecurity program goes into effect the moment the organization is called upon to respond to a security event.
Incident Readiness

The absolute worst time to determine whom to call and what to do is after a compromise has been identified. Aside from the obvious repercussions of a threat actor having access to your most sensitive data and systems, companies need to consider the legal, regulatory, reputational, and financial impacts of an incident. Any delay in incident response could pile on ramifications, including allowing the adversary to further his attack, to losing evidence that might be crucial during a court case, to failing to meet regulatory requirements which result in larger-than-anticipated fines. If your organization has purchased cyber insurance, your provider will also want to see procedures (starting with implementation of technology and controls, through incident response) followed accurately and in a timely fashion; absent this chain of custody, any outside financial assistance could be lost as well.

The point of this section is not to spread fear, uncertainty, and doubt. Rather, the key takeaway should be that your company has an opportunity to build an incident response ecosystem that is ready to spring into action when called upon to do so.

Regardless of a company’s size or capabilities, external experts can ease the pain of incident handling. Professional incident handlers spend their days, not coincidentally, handling incidents, whereas traditional security teams are primarily focused on keeping operations running smoothly and malicious adversaries away from the network. Therefore, it is often helpful to have a set of incident responders “on call.” These individuals can include law enforcement (local police and FBI), forensic investigators, external legal teams, and backup and recovery providers. If you’ve adequately prepared to manage an incident, relationships with these resources will have been forged ahead of time. Doing so presents several benefits: In the heat of the moment, having the name and number of your local FBI agent is quicker and more effective than trying to dig one up. A forensic investigator who knows your organization, the type of systems you use, and the people involved will be able to act quicker than someone who must start from scratch without any prior knowledge of internal systems and abilities. An external legal team can not only provide an alternate point of view during an incident, but they may be subject to different disclosure obligations than your internal team, which could prove vitally important when or if negligence becomes a question.

For more information, visit LBMCInformationSecurity.com or call 1 (844) 526-2732
Establish your incident response network and contractually retain the necessary services.

Your internal and external teams will act jointly on the first three and final bullets, while you'll need to largely depend on partners for recovery. Many companies are so focused on ensuring containment, eradication, and recovery that they forget the importance of reviewing the incident for lessons learned. This final step is essential because it will allow the organization to be better prepared for the next event:

- What did we miss?
- What did not run as smoothly as anticipated?
- What resources were not mapped appropriately?
- What went particularly well?
- What can we learn from one area of the process to improve another?

A post incident activity checklist may be useful here, as will your outside partners. Incident responders are not only functional during an event, but they can help your organization before and after as well. Remember, incident responders handle incidents every day, whereas you—hopefully—do not. Some firms might think it's “waving the white flag” to lean on incident responders, but really, it's just good preparation, and will ultimately improve all aspects of your security program.

Once you have your network and internal resources defined and able to respond, the next steps of incident response are:

Detection & Analysis

Containment

Eradication

Recovery

Post-Incident Activity
External incident responders can further help companies prepare for an incident through organized tabletop exercises. These exercises are designed to emulate real-life situations (based on the expert’s past work) and allow your company to practice an incident without having to suffer through a real one. Just like you would not decide to run a marathon without proper training (putting in “X” miles per day/week/month, running in different climates and on various terrains), equipment (comfortable, supportive running shoes and clothing that doesn't chafe), and nutrition (eating the right balance of healthy food), you should not think your company can jump into handling an incident without adequate training. Tabletop exercises will allow you to understand your strengths, weaknesses, opportunities, and threats (SWOT analysis), identify common but hidden “gotchas” (such as how your HR department stores PII or transmits e-PHI to the company’s health insurance provider unencrypted), and build a better relationship with your provider. Thus, when a real incident is declared, neither party is walking in blind; every team can fire on all cylinders from the very start.

A large part of the success in responding to an incident is your extended security team.

No organization can do it alone. Incident responders have relationships with law enforcement, forensic specialists, law firms, etc., and vice versa, that will be a boon to your internal security team. Consultants provide an outside-in perspective about your organization and use their extensive knowledge of and hands-on experience with vulnerabilities, threats, weaknesses, and adversary tactics that let your company prevent, detect, and respond to security issues before they become incidents. Contrary to some organizations’ beliefs, having relationships with dedicated specialists in place and testing them from time to time with mock incidents will speed up and improve response capabilities significantly. You will likely learn quite a bit about your day-to-day security operations through these external relationships and be able to provide continuous improvement to other parts of the security program as well.
Conclusion

Every day we read news of a new data breach.

What can we do?

In today’s data-intensive world, an organization’s ability to secure its people, processes, and technology (including the supply chain and third-party partner ecosystem) while maintaining compliance is as instrumental to running a successful business as managing finances or selling valuable, trustworthy products.

Yet information security programs have not caught up with the growing demands of collecting, governing, and storing mass amounts of data.

Data breaches and security incidents are common because organizations continue to add data to digital repositories while neglecting to take basic security precautions.

As cybersecurity has entered the limelight, it’s become easier for organizations to convince boards of directors that increased funding for the security program will help. Without proper implementation of critical controls and processes, however, no amount of budget will stop cyber criminals. Companies must be as dedicated to staying in front of threats as cyber criminals are to finding and exploiting vulnerabilities.
Your Security Program

This means developing a holistic security program that is proactive and risk focused. Vulnerability management helps set the foundation, allowing organizations to continuously assess areas of strength and where improvements are mandatory. From that baseline of understanding, it’s then vital to build an incident response program that prepares the organization to handle future security incidents. A key element in this preparedness is knowing adversary behavior: what motivates cyber criminals, tools and tactics that may be used, and how to quickly detect (and react) when malware or other forms of compromise are found.

Your company’s ability to respond to and mitigate an attack is just as important as your proactive capabilities. The damage from a mishandled compromise could be greater than the initial incident itself.

**Staffing your IT and security teams with dedicated experts is therefore a key element of any security program.**

Some organizations may be able to accomplish this entirely in-house, but most cannot; even the best-resourced organizations understand the importance of an outside network. Outsourced services not only provide a deep level of expertise and distinct perspective, but additionally free up your team’s time to focus on high-level strategic initiatives and processes rather than managing technology. In the long run, leveraging outside experts will save you time and money, and better prepare your company to handle the myriad cyber threats that affect organizations every day.
Extend Your Team

LBMC Information Security

Running a successful business requires removing known obstacles from your path. A well-designed information security program provides critical intelligence about risks, allowing you to make better, faster decisions about your organization’s future. While no organization can eliminate 100% of cybersecurity risks, working with an expert team reduces risks, mitigates threats, and helps maintain compliance.

LBMC Information Security reaches beyond security infrastructure and protection to help make your overall security operations more effective and efficient, preparing you for the worst, but helping to keep incidents at bay.

As leaders in the information security industry and honored recipients of numerous awards, LBMC professionals place a unique depth of expertise at your disposal. Most importantly, we provide independent appraisals for a true and objective assessment of your security environment. 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.