CIMPHONI WHITE PAPER SERIES

Building a Cyber Fortress to Protect Your Digital Assets

Dr. Max Boedder

cimphoni

Data is the new currency of crime, and the growth of mobility, cloud computing, "bring your own device" policies and the Internet of Things (IoT) open new attack vectors for cyber criminals. Hackers often are well-trained and well-organized criminals, not just loners with tech skills who decide to break in because they are bored. If your top executives are not making cybersecurity a top priority in your organization, they are making a critical business mistake. High-profile security breaches at companies like Sony Pictures, Home Depot, and Target have generated negative headlines, but the impact is much more than the PR headache. According to PricewaterhouseCoopers, the number of detected incidents in 2014 was almost a 50% increase over the prior year, and the average financial impact per incident was $2.7 million.

There are basic steps that every company should take to significantly improve their cybersecurity posture without breaking the bank. For companies with significant digital assets, it is essential to build a cyber fortress to protect these assets. There are some common vulnerabilities that can be addressed with minimal effort on the part of your IT team.

Common Vulnerabilities and Baseline Defense

Most cybersecurity exploitations of vulnerabilities have the same root causes:

1. Outdated patch levels: New vulnerabilities are discovered daily and manufacturers of operating systems and other software frequently release patches to remove such vulnerabilities. Organizations should be aware of newly released patches and deploy them as soon as possible, but not before testing them. Also, be sure to update all systems. Sometimes patches are not applied to some systems for a variety of reasons, which unnecessarily will leaves them open to vulnerabilities.

2. Network misconfigurations: Poorly designed network configurations can also leave many "back doors" open for exploitation. It is important to make sure that only needed protocols, services and ports are open and active. If there is not business need to expose these interface points, they should be disabled. It is a good investment of time and a best practice to periodically review network and server configurations accordingly.

3. Anti-virus and anti-malware programs: Anti-virus and anti-malware programs are basic, and yet very important, security controls to have in place. You should ensure that all servers and end-user computing devices, like desktop computers, laptops and tablets have anti-virus software installed. Similar to patches, you want to make sure that all systems with anti-virus software have the latest virus and malware definitions. Without the most current definitions, you will not be protected from the latest threats.

4. Detective Controls: As a general rule, every preventive control should have a detective control behind it. This will allow you to detect potential failures of preventive controls. For example, behind a firewall (a preventive control), you should place an intrusion detection system (a detective control).

In many cases, the only way to detect unwanted activities is by examining system logs, another detective control. You want to store your logs in a secure location where they cannot be altered. Remember that hackers like to erase their trails and will attempt to modify your system logs to hide their presence and activities. System logs need to be analyzed and cross-referenced to detect unusual and unwanted activities. There are service providers in the market that will store your logs in the cloud and automatically analyze them based on common patterns. In many cases, such log aggregation and automated analysis can be your primary control for detecting cybersecurity incidents.

5. Training: Too often IT and cybersecurity staff are not properly trained on the tools and security controls assigned to them. Staff may not use them properly or may only take advantage of basic features, neglecting advanced features and leaving the company at risk. The best tool and security control cannot protect you if your technical staff is not trained to use them properly or fails to fully utilize their capabilities.

Even after implementing these five basic defenses, most organizations are not fully protected and need to do more. The Five Pillars of Cybersecurity, when properly implemented, will provide an effective cybersecurity program. They address the following areas: the human "firewall", system updates, defense in depth, protecting sensitive data and incident management and response.

The Human Firewall

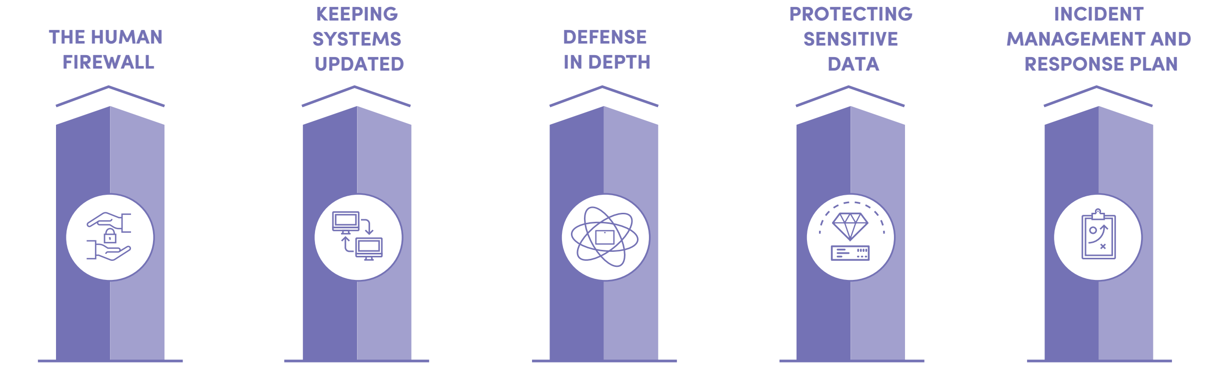
The weakest link in many security systems is often the human element, as untrained or careless employees unknowingly open the door to hackers. A common phrase in the hacking community is "amateurs hack systems, professionals hack people." A social engineering hack is a non-technical kind of intrusion that relies on human interaction and often involves tricking people into breaking normal security procedures. Hackers may rely on employees' helpfulness, exploit their weaknesses like vanity, appeal to authority or eavesdrop. Employee awareness and training programs can go a long way to protecting your organization by building up a "human firewall."

Social Engineering: Amateurs hack systems, professionals hack people

Phishing is a particular kind of social engineering hack where an intruder tries to gain access to a network or system by pretending to be a reputable entity or person, often via email. According to the Verizon 2015 data breach investigations report, 23% of recipients open phishing messages and 11% click on attachments. We recommend providing phishing awareness training to all employees.

Other safeguards to improve the human firewall are applying need-to-know and least-privilege principles as well as separation of duties. The need-to-know principle dictates that employees shall have access to only the information that they need to perform their job duties. A stricter implementation is that they only have such access at the time they need to know it. The least-privilege follows essentially the same approach, but extends to programs and processes.

PILLARS OF CYBERSECURITY PROGRAMS



THE HUMAN FIREWALL
Provide phishing awareness training; apply need-to-know and least-privilege principles; separation of duties

KEEPING SYSTEMS UPDATED
Keep systems and applications up to date and deploy patches regularly

DEFENSE IN DEPTH
Build multiple layers of security

PROTECTING SENSITIVE DATA
Identify mission-critical and sensitive data and concentrate them at a few data centers and locations within those data centers

INCIDENT MANAGEMENT AND RESPONSE PLAN
Conduct an exercise to prepare for a cybersecurity incident

Separation of duties or segregation of duties requires that for certain business processes, more than one person is required to complete the process in order to prevent fraud. Implementing these principles can improve the effectiveness of your security program without requiring a significant investment.

Keeping Systems Updated

Some executives and CIOs would be surprised to find out how many old and outdated system and application versions they are still using, residing on PCs, laptops and servers. Old versions of systems and applications often present old and well-known vulnerabilities to hackers. Unsupported systems and versions can be even more vulnerable. Hackers love to encounter these, as the methods to breach them are well known in cybercriminal communities. Our advice is to keep systems and applications up-to-date and to deploy patches regularly.

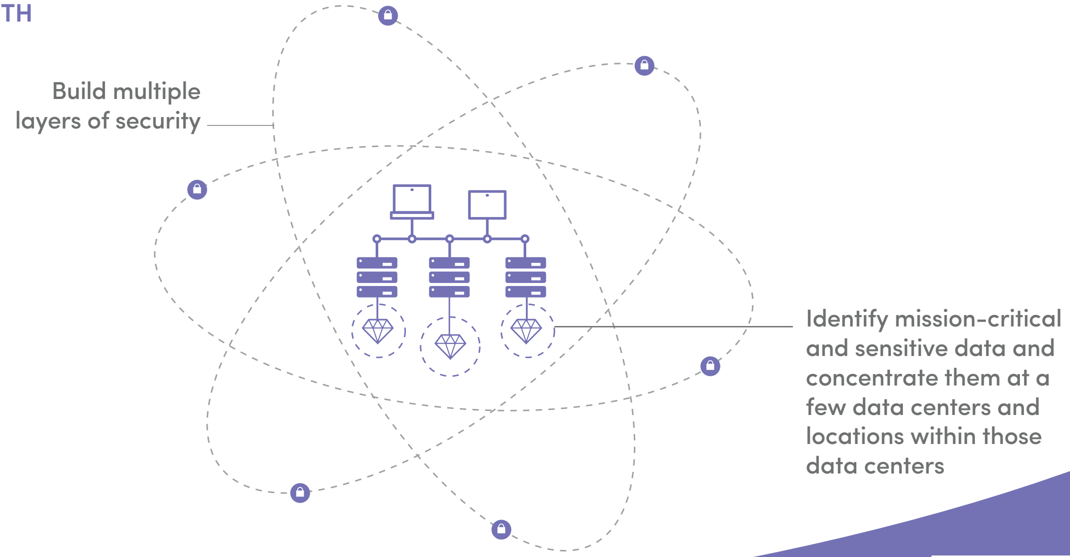
There are tools available that will scan your company's networks, servers and applications to identify these vulnerabilities and outdated versions. These tools employ the Common Vulnerability Scoring System (CVSS) to convey the severity of identified vulnerabilities, which will help you prioritize your remediation efforts. Running a scan on your network can give you a good idea of how vulnerable you are, and where to focus first on reducing your risks. This is often the starting point in many cybersecurity remediation programs.

Defense-in-Depth

The term "defense-in-depth" refers to building multiple layers of security, rather than just one layer of defense to the outside, such as a perimeter firewall. If you picture a medieval castle, you will think of an outside wall around the entire castle, along with a moat. Access to the castle was controlled through a few guarded gates with drawbridges across the moat. Somewhere inside the castle, beyond the outer courts, may be another tall wall with a few gates and guards. This second wall might protect the inner court. Inside the inner court may be a third wall with perhaps only one gate that is guarded by elite soldiers. Inside that wall would be the king's court. Similar to these multiple walls to protect important parts of the castle inside, a defense-in-depth approach applies multiple layers of security and controls in corporate networks.

As an example, you may protect a web server by a perimeter firewall, then a demilitarized zone (DMZ) in your network, followed by an internal firewall, then the use of an intrusion detection system (IDS), followed by a web

DEFENSE-IN-DEPTH


Build multiple layers of security
Identify mission-critical and sensitive data and concentrate them at a few data centers and locations within those data centers

application firewall (WAF). This gives you multiple layers of defense and a potential attack would have to pass through all of these layers in order to get to your sensitive data.

Beware of "all-in-one" or unified threat management (UTM) security devices that perform all of the layers of defense in one device: if a hacker is able to compromise the device, now all layers of defense are compromised at once. This defeats the purpose and the additional protection of a defense-in-depth approach.

Protective Sensitive Data

An adage in cybersecurity is, "there are two types of companies – those that have been hacked and those that don't yet know they have been hacked." As complex multi-stage and compound attacks have become much more common, it is prudent to assume that, sooner or later, some hacker will be able to breach an organization's network. This school of thought is known as the Assumption of Breach (AoB).

> "There are two types of companies – those that have been hacked, and those that don't yet know they have been hacked."

As a result, more and more organizations identify mission-critical and sensitive data – the crown jewels – and concentrate them at a few data centers and locations within those data centers. This approach affords additional efforts to protect these data assets by building a Fort Knox around them. In other words, even if hackers are able to break into the corporate network, the goal is to prevent them from getting to the crown jewels. Some people liken this approach to a pomegranate, which has a hard shell on the outside, is soft in the inside, and then has some very hard seeds distributed inside of it. This approach is an extension of the defense-in-depth model. Rather than trying to apply a broad security blanket, it focuses efforts in a cost-effective manner and, thereby, provides a stronger security posture to protect a firm's most important data assets.

Incident Management and Response Plan

Once you put your basic protection and controls in place, you want to conduct an exercise to prepare for the worst: a cybersecurity incident. Much like a military battle plan, this can be a tabletop exercise where the participants sit in a room and perform a dry run of what they would do in the case of an actual cybersecurity incident. As you repeat these exercises, the incident scenarios should become progressively challenging.

You may want to start out with a simple situation that presents itself as a false alarm, and then increase the severity into full-breach incidents with multiple stages of events over a longer period of time. It is a good idea to engage an external expert to provide the incident scenario and to facilitate the tabletop exercise without any of the participants having prior knowledge of the scenario. This ensures both a realistic scenario and realistic behaviors by the incident response team.

In order to run an incident response exercise, you must develop an incident response plan (IRP), which defines the members of the incident response team and their actions, based on how an incident would unfold and the associated actions that need to be taken. The team should include not only IT staff, but also members from all impacted departments. This includes operations or lines of business, Legal, Risk Management, Human Resources and Public Relations. It is important that these team members make themselves available for the exercise and participate according to the IRP.

The main objectives of an incident response exercise are to practice and test the effectiveness of your incident response plan, to identify and improve weaknesses of the plan, and to train your staff on the plan. However, as a side-effect, a properly conducted incident response exercise with members from other departments can dramatically increase your organization's awareness of cybersecurity and potential impacts of a weak cybersecurity program. That increased awareness may help you with cooperation, staffing and funding.

Advanced Controls

Once you have taken care of the basics, put fundamental controls in place, trained the staff and conducted an incident response plan exercise, it is time to look into some more advanced controls. These controls may differ depending on your organization. When developing your cybersecurity program, keep in mind the famous Pareto principle or 80/20 rule often applies: 20% of your security program may consume 80% of the resources and costs. Therefore, you will need to be deliberate about next steps.

> 20% of your security program may consume 80% of the resources and costs.

- **Vulnerability and Hardening Scans:** A good next step might be to conduct periodic vulnerability scans, both external and internal. The more frequently you run these scans, the sooner you are aware of new vulnerabilities and can remediate them. A recommended minimum is once a quarter but a best practice is to scan weekly. Additional scan tools are available to ensure that server and network devices are hardened and only allow the applications, ports, and protocols that are required to run the business.
- **Code analyzers:** If you are developing custom applications, consider a code analyzer to detect security vulnerabilities.
- **Lockdown of Workstations:** Desktop and laptop computer workstations should be locked down to prevent unnecessary software from running on them. For example, many organizations do not allow the use of USB flash drives in order to prevent the introduction of malicious software. Also, many organizations remove "administrator" rights from most users to ensure they do not intentionally or unintentionally install unauthorized software that may contain malicious code.
- **Web-filter and Email Scans:** Web filters block access to web sites that are not business related and may infect your systems such as online gambling web sites. Similarly, email scanners block or quarantine emails with potentially malicious attachments that could infect your systems.
- **Phishing Campaigns:** After employees have completed phishing training, we recommend following it up with external phishing assessments by a third party. These assessments simulate a phishing attack and try to trick your employees into opening an email attachment or clicking on a hyperlink. This external assessment lets you know how susceptible your employees are to real email phishing attacks. If you don't do it, the hackers will!
- **Data Loss Prevention (DLP):** DLP tools prevent certain types of confidential data from either intentional or unintentional transfer to locations outside of your network. For example, DLP tools might scan outbound emails to ensure that no credit card data or social security numbers are emailed outside the company. Other DLP tools may prevent users from copying and pasting this type of data on their workstations.

ADVANCED CONTROLS

- Vulnerability and Hardening Scans for Servers and Network Devices
- Code analyzers for custom applications
- Lockdown of Workstations
- Web-filter and Email Scans
- Phishing Campaigns to Test Employee Vigilance
- Data Loss Prevention (DLP) for servers, workstations, and network egress points
- Penetration Tests
- Detection of Rogue Wireless Access Points
- Use of Strong Passwords and Strong Encryption

- **Penetration Tests:** At least once a year and after any major changes, you may want to conduct a penetration test. Essentially you hire ethical hackers or "white hat" hackers to attempt to break into your network without causing any damage. These ethical hackers will exploit vulnerabilities and use their skills to overcome or bypass the controls you put in place. The result of these penetration tests can identify vulnerabilities that you might not find otherwise.
- **Wireless Access Points:** Do not forget to also conduct wireless penetration tests to find out if your wireless network has vulnerabilities that hackers could potentially exploit as another entry point into your network.
- **Passwords and Encryption:** Strong passwords that are difficult to guess, are not written down anywhere, and change frequently are an important safeguard to prevent unauthorized access to your systems. Wherever you apply encryption to make sensitive data unintelligible, make sure you are using strong encryption algorithms and you keep the encryption keys well protected. The strongest encryption algorithms do not protect your data if you do not have a solid key management process in place.

There are additional advanced controls that may make sense in your computing environment. These controls included hardening of servers, network devices, and workstations, file integrity monitoring (FIM), and two-factor authentication for virtual private network (VPN) access from the outside of your network and for privileged users.

The next generation of cybersecurity protection products are using artificial intelligence and machine learning to detect suspicious user or machine behavior and suspect code. So-called zero-day malware is a new virus or other malware for which there are no detection patterns or signatures available yet. Products that employ artificial intelligence can detect and protect from such zero-day vulnerabilities where traditional products do not.

Determination of next steps and appropriate advanced measures to be taken depend on various factors, including your organization's threat landscape, your crown jewels, your budget, and the current status of your cybersecurity program. Threats continuously evolve and so do advanced security measures. If you are not sure which advanced measures are right for your organization, engage a trusted cybersecurity expert to guide you through the process.

CREDIT CARD DATA AND THE PCI STANDARD

One additional cybersecurity requirement applies if your organization stores, process or transmits branded credit cards including Visa, MasterCard, American Express, Discover and JCB – you are subject to the Payment Card Industry Data Security Standard (PCI DSS). The PCI Security Standards Council defines and evolves the PCI DSS standard. The current standard, as of April 2016, is 3.2 and is available for download at the PCI website.

The PCI DSS has 12 requirements with over 250 sub-requirements. Depending on the type and number of transactions that your organization processes each year, there are different merchant levels for compliance. Merchants at level 1 (over 6 million transactions per year) require an external audit by a qualified security assessor (QSA). Merchants at level 2 (1 to 6 million transactions), level 3 (20,000 to 1 million transactions) and level 4 (less than 20,000 transactions) are required to complete a self-assessment questionnaire or to self-certify compliance.

Obtaining PCI DSS compliance can appear to be a daunting task. A particular challenge can present itself when an organization grows its volume of annual transactions that places them into a higher merchant level. Companies that become a level 1 merchant through though organic growth, acquisitions, or simply because its customers prefer payment by credit or debit card, need to conduct a formal review of PCI DSS and certify compliance via an Attestation of Compliance (AoC) with evidence of compliance documented in a Report on Compliance (RoC).

If the company has been interpreting the PCI DSS generously when an internal self-assessment questionnaire was adequate to demonstrate compliance (levels 2, 3 and 4), the findings of the QSA may come as a shock. A PCI DSS remediation project to bring the organization into compliance can be a costly and resource-intensive, enterprise-level project. Organizations that are not compliant can be fined, sanctioned or even lose the ability to process cards.

Being PCI DSS compliant does not mean that an organization has an excellent security posture. The standard is a minimum requirement and applies only to credit card data. Your organization may have other crown jewels or important digital assets worthy of protection such as personally identifiable information, protected health information, as defined by the Health Insurance Portability and Accountability Act (HIPAA), financial data or intellectual property. Becoming PCI DSS compliant can be an excellent foundation and starting point for an effective enterprise-wide cybersecurity program.

Organizational Models for Effective Cybersecurity

Effective cybersecurity starts at the top of the organization, with the board of directors and C-level executives. These leaders must determine the risk appetite of the organization and set expectations for the alignment of the cybersecurity program with business objectives.

Regardless of the organizational structure, a major focus is the alignment of cybersecurity with business objectives.

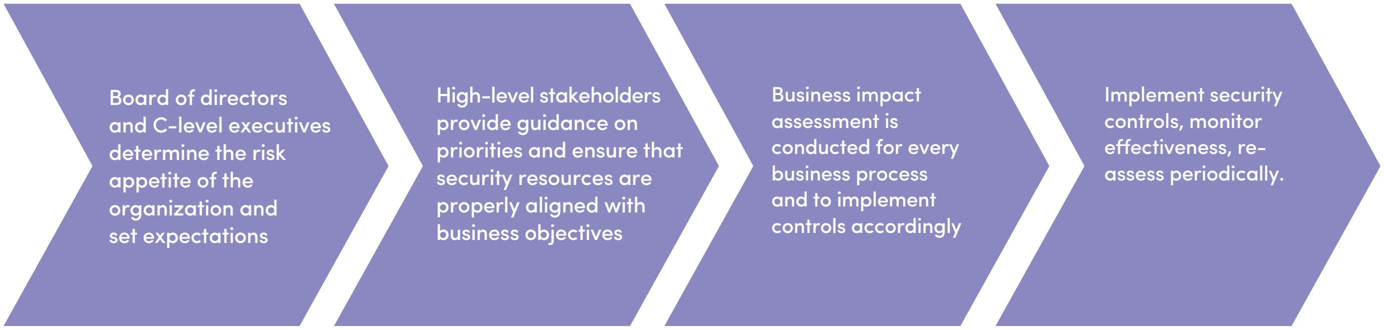
Typically, this is accomplished with a steering committee that meets regularly, preferably once a month. It can also be included as part of the scope of the Enterprise Risk Management Committee. High-level stakeholders from across the enterprise provide guidance on priorities and ensure that security resources – people, processes, technologies, and budgets – are properly aligned with business objectives. Without this alignment at the top, cybersecurity results may be less effective than desired and may place unnecessary burdens on business activities.

Next, a business impact assessment is conducted for every business process to determine the recovery time objectives for the longest acceptable down time due to a cybersecurity event, and implement controls accordingly. In addition, there may be regularly scheduled tabletop and actual incident response and disaster recovery exercises.

In a perfect world, the organization will have a Chief Information Security Officer (CISO) who reports directly to the board in order to avoid potential conflicts of interest. However, this is not feasible in every organization due to the size and scope of the company. In any case, a full-time CISO is ideal, as it ensures a dedicated leader to manage business alignment and ensure the implementation and ongoing operation of a cybersecurity program. The CISO will also ensure the organization stays up to date on managing the latest cyber threats, implementing controls and assessing the effectiveness of the controls.

Many organizations may not have a CISO and the responsibility for cybersecurity is assigned to someone in

ALIGNMENT OF CYBERSECURITY WITH BUSINESS OBJECTIVES



Board of directors and C-level executives determine the risk appetite of the organization and set expectations

High-level stakeholders provide guidance on priorities and ensure that security resources are properly aligned with business objectives

Business impact assessment is conducted for every business process and to implement controls accordingly

Implement security controls, monitor effectiveness, re-assess periodically.

the IT department who has a small team, or no team at all. These organizations often opt for a two-phased approach to an effective cybersecurity program. The first phase is a transformation from the status quo to an effective security program that includes standard security operations, risk-based areas of focus with implementation of additional controls, and an alignment with business objectives. This process can take between six and 18 months.

In this situation, an experienced interim CISO or a cybersecurity consulting firm may be the best choice to take the organization through this transformative process. Depending on the size of the organization, a seasoned security program manager or project manager may also be required to manage the detailed implementation tasks of the program and project budget.

As a second step, a permanent CISO will take over the implemented cybersecurity program and lead it going forward. The permanent CISO will need to closely assess the threat environment of the organization, adjust the security posture of the firm to evolving threats, and maintain alignment to the business strategy.

Some companies may not have the need or budget for a full-time CISO, yet need a seasoned leader for their security strategy and implementation. Somebody within the IT organization or the risk management organization may perform CISO duties as a secondary job function, but conflicting priorities are often a problem that can leave the organization's sensitive data at risk. One solution is a virtual CISO who performs similar duties for several companies on a part-time basis. The virtual CISO brings the knowledge and experience of a seasoned CISO at a lower cost, while also ensuring that a dedicated resource is focused on your cybersecurity program.

If you are struggling to get sufficient resources in your organization to fund the cybersecurity organization that you need, it may help to educate executive management on the importance of having an effective cybersecurity program in place using business and risk management concepts such as:

- Probability of attacks and other incidents
- Costs of potential loss of business and brand impact
- Cost-benefit analysis of risk mitigation measures
- The need for regulatory and contractual compliance

However, such education does not necessarily guarantee additional staffing and funding.

Protect Your Organization

The recent cybersecurity breach at a large internet company where at least 1 billion user accounts were hacked was not discovered until two years later. According to former employees, security was pushed to the back end of priorities at the time. In the digital age where data is the new currency of crime, the importance of an effective cybersecurity program should not be underestimated.

If your organization is concerned about the strength of its cybersecurity program and the risk of a breach, we encourage you to consider the steps described above. Effective cybersecurity does not have to break the bank, but just one data breach can bring down your entire organization.

ABOUT THE AUTHOR

Dr. Max Boedder, Partner

After receiving a Master's degree in Computer Science, Max started his IT career in software development. From there, he transitioned into the business process outsourcing (BPO) industry, where he held several senior and C-level positions before he returned to IT consulting. Max also holds an MBA from Webster University, a Doctorate in Business Administration from the University of Phoenix. He is a Certified Information Systems Security Professional (CISSP) as well as a Certified Information Security Manager (CISM). Max is an eight-year veteran and former officer of the German Air Force. He likes spending his spare time in the gym where he studies several martial arts.

About Cimphoni

Cimphoni is built on the premise that technology, when properly applied and led, can deliver innovative solutions that transform businesses, enrich the products we use daily and improve the quality of our lives. The Cimphoni team is comprised of highly experienced technology and business leaders with a thirst for innovation and a passion for solving problems. Founded in 2012, we serve customers throughout the United States from our offices in suburban Milwaukee.

P.O. Box 80
Hartland, WI 53029

t: (888) 470-0448
e: info@cimphoni.com

www.cimphoni.com

Contact Cimphoni

If you would like to enhance your cybersecurity program, please contact us at (888) 470-0448 or info@cimphoni.com. We can help you mitigate risks and build a cyber fortress around your organization and its most critical data.