Five Steps to a Successful Cybersecurity Program

Any organization that relies upon wide-area networks for communications and connectivity, is not just susceptible to security attacks, they will most certainly be a target for those attacks. The big question is, how well will they handle the attacks, to prevent them from becoming a security breach? The most reliable and successful means to prevent security breaches is having a successful cybersecurity program.

An effective cybersecurity program requires a three-pronged dedication to empowering people, implementing processes, and deploying technologies. Together, this triad establishes a value chain that accomplishes much more than each element working independently. Through implementing best practices, they can lead to a successful cybersecurity program.

Employing the five steps outlined in this white paper, with the effective utilization of people, processes, and technology, Mosaic NetworX demonstrates a case where the whole is greater than the sum of its parts.

The Mosaic managed cybersecurity service is built on best practices. It is strategically designed to simplify the utilization, integration and interactions of the people, processes, and technologies, that support a cybersecurity program to deliver effective results.

Whether your organization needs to create a cybersecurity program from scratch, or strengthen an existing program, these five essential steps are necessary to ensure a successful outcome.

Mosaic NetworX Managed Cybersecurity Services

Mosaic NETWORX

sales@mosaicnetworx.com • www.mosaicnetworx.com • 800.688.3770

How to Begin?

The first question is, do you have a cybersecurity program in place today? We understand you may not be cybersecurity experts. You may in fact, have security personnel in-house. But, as we mentioned in the introduction, cybersecurity requires people, processes, and technology. It also requires ongoing training and reassessments of best practice implementation of all three areas. This is where Mosaic comes in.

Mosaic NetworX Managed Security Services (MSS), includes professional services offered by our Information Security Group (ISG). Mosaic has a vast set of diverse resources and skillsets, proven processes, and technology solutions that are continually evolving to stay ahead of the ever-changing security requirements. The result is quality execution on the in-depth cybersecurity program assessment findings and subsequent remediation. We have the capabilities you need to harden your defenses, and put measures in place to help your organization become more resilient, shore up security gaps, and eliminate threat vectors.

The Five Steps

1. Cybersecurity Risk Assessment

Though there are scores of technologies and strategies that address cybersecurity, without an assessment, they are all rendered less effective, and in some cases, useless. When it comes to security, trust can be a vulnerability, while control is a strength.

"Security leaders are under a lot of pressure to show quick wins while knowing full well that everything they do will be heavily scrutinized and challenged, and ultimately, they will pay the price for things that are not under their control." - *Yaron Levi*

A cybersecurity assessment includes the process of identifying, analyzing and evaluating risk. This includes determining key areas of risk, controls, and recommended remediation for any gaps in controls. A cybersecurity risk assessment provides the framework for determining and remediating security vulnerabilities within the IT environment, workflows, and user awareness.

Cybersecurity is as necessary as an annual physical. This cyber "health check", provides the framework for subsequent actions to be taken. This is the most effective tool in the cybersecurity tool-kit to justify the requirement for any security products and services. Most decision makers are data-driven, and the assessment is a comprehensive examination of your IT environment, workflows, and user awareness of cyber threats. However, cybersecurity impacts far more than IT, and assessment findings should be shared among key constituents, including the highest-level business executives and other key stakeholders.

Mosaic Cybersecurity Risk Assessment Elements

Physical Security Network Management & Monitoring	• Review of management and monitoring tools required to maintain a secure network firewall • Review firewall implementation, including rules, monitoring and ongoing assessment of vulnerabilities
Malicious Code & Spyware	• Antivirus systems are reviewed, including desktop PCs, servers, email, web and FTP systems
Host Security – Servers	• Servers are the core computing infrastructure in most organizations and contain sensitive information (e.g. user credentials, customer details, financial and human resource records, etc.)
Host Security – Workstations	• Elements of workstation security are reviewed
Network Intrusion Detection / Prevention System	• The testing team will assess the placement of network sensors and overall design, detection ability through active log analysis, and incident response procedures
Authentication & Access Control	• The methods of establishing a user's identity on the network are assessed
File System Security	• The Cybersecurity Assessment examines file system components to ensure the security and integrity of the documents
LAN Infrastructure	• The Cybersecurity Assessment focuses on layer 2 security and access control, the secure management of switches, routers, etc. It reviews protocols and transports, DNS and DHCP security, secure use of SNMP, RMON and other network management protocols, access controls, and virtual LANs)
WAN Infrastructure	• Cybersecurity Assessment focuses on the secure management of switches, routers, reviews protocols and transports, and the security of 3rd-party connections, such as partner networks, encryption, access controls and virtual LANs
Wireless Security Review	• A review of the wireless network infrastructure is conducted
Remote Access	• Examines various components that provide remote connectivity from mobile workers, home offices and small branch offices not equipped with permanent wide area connections
Vulnerability Assessment	• An examination of the current vulnerability assessment practices and procedures, vulnerability assessment tools, incident response and reporting, escalation procedures, and regular reporting is conducted
IT Policies and Procedures	• The organization's policies and procedures are reviewed and compared against industry and vendor best practices. The review also includes the organization's ability to monitor and enforce the rules defined in each policy and procedure
IT Operations	• Thoroughness and organization of the network documentation will be reviewed. The greater security concern associated with sensitive documentation is the proper encryption of data at rest (storage), and in transit (over the network)
Observation & Recommendations	• From the data gathered in the analysis of the assessment, specific observations and recommendations are documented. In some cases, these remarks will be based on industry best practices
Reporting	• Executive Summary – a high level overview of findings, recommendations and comments on the overall effectiveness of the network • Technical Review – intended for IT Executives, highlighting specific technical findings, observations and recommendations • Risk Assessment Tabular Report – tabular listing of risk areas, overall risk rating, and remediation steps • Appendices – review of methodology, documents reviewed, and interviewees

2. Security Remediation

Security remediation is where the results of the cybersecurity risk assessment are applied. Included in the remediation plan where applicable, will be SD-WAN. There are several remediation solutions, including setting up patch management, firewall fixes, application of new technology, and user training.

Remediation of security vulnerabilities must be addressed by all organizations in advance of hackers exploiting their weaknesses. Effective remediation involves multiple, continuous processes that together, provide management with the ability to foresee and address problems, before an attack occurs.

Remediation services include a comprehensive plan for the information security issues and/or modifications that need to be adopted. Mosaic security experts address the essential operational changes required, and work directly with the individuals involved in the process.

A remediation plan enables the security team to determine the most important issues that need to be addressed, based on the company's goals. This goes beyond the assets it needs to protect, and formulates the most appropriate path going forward.

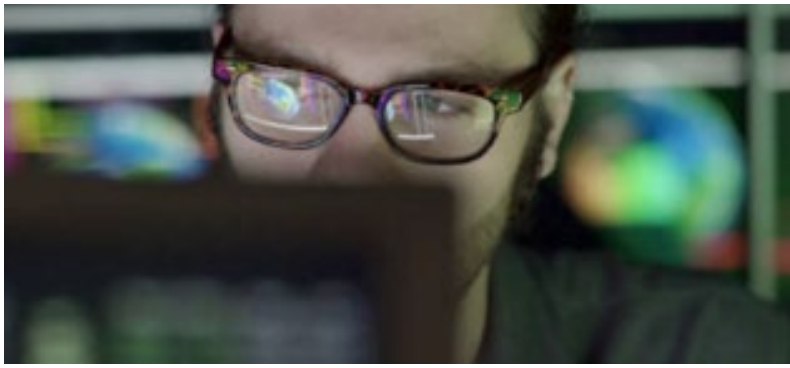
Information Security (IS) managed services provide comprehensive compliance and risk management. Mosaic IS remediation services include:

- Compliance audits
- Consulting and implementation
- Implement cybersecurity best practices
- Professional services

3. Security Awareness Training

Cybercrime is extremely sophisticated. When it comes to phishing, ransomware and social engineering attacks, your employees, whether they know it or not, are on the front lines of a cyber battle that can have significant repercussions for your business.

Your employees are exposed to complex social engineering attacks, and therefore, your organization is exposed, and needs an effective approach to successfully manage this problem. The Mosaic security awareness training program is a comprehensive approach that integrates baseline testing to understand the current level of risk among your users.



Providing an additional layer of security, security awareness training represents a "human firewall". Many breaches occur as the result of phishing attacks and employee behavior, whether unintended or intentional, and must be addressed through

security awareness training. Many industries require companies to establish policies that necessitate employees pass security training and certification.

Organizations within different industries have discrete risk profiles that can be mitigated through security awareness training. The Mosaic Automated Security Awareness Program (ASAP) tailors the most effective security awareness training for our customers, based on their industry, and the markets they serve.

As threat vectors continue to grow and evolve, dedicated security risk training becomes more important than ever, and is a vital and necessary part of the corporate culture. As security programs are planned and executed, they typically go one of two ways. Either the program will be successfully adopted, growing and evolving as needed, or the program will fail. A program that works one year, is not necessarily going to work the next year. As regulatory requirements and the threat landscape continues to unfold and broaden, the security awareness training should adapt to meet those changes.

It is important to consider how your organization's security program should mature and develop a year from now. While it can be a challenge to transition from having no security program in place, to becoming an industry leader in a short period of time, a well-designed security awareness program can help you achieve that goal. Mosaic allows you to select the level of maturity for your specific security awareness program to achieve over a 12-18-month period.

Security awareness covers several different domains, such as industry compliance requirements, physical security concerns, and a user's behavior behind the keyboard. How a user reacts when faced with a security risk is a critical part of an organization's security posture. With 180 different cybersecurity training modules, Mosaic provides the proper training and simulation of attacks that greatly increase the chances for users to act favorably when a real threat ensues. Mosaic customers select user behaviors from the supplied list that are most important to their organization. Mosaic helps guide customers in choosing these behaviors. Studies show that it is most effective to focus on changing 2-3 behaviors over a 12-18-month timeframe. If you try to train users on every behavior all at once, they tend to retain very little of the new knowledge.

Mosaic offers over 180 training courses. Interactive training is delivered through training modules that users must complete. These modules are typically 15 minutes or less, though some can be longer and more detailed. It's important to consider the culture of your organization, and the best method for delivering security awareness training and related information to users. Your security awareness program should reflect the unique culture of your company. It is best to select the styles of training that will most appeal to your organization and its users.

Security awareness training may need to accommodate users who speak different languages, or live in different countries. Mosaic offers security awareness training modules in different languages to accommodate your diverse business needs.

Role-based training can help bolster the confidence of employees by focusing specifically on the threats that affect them. Select as many modules as you need to make your security awareness training thorough and complete.

Mosaic facilitates regular phishing tests that allow your employees to practice the skills they've learned as part of their security awareness training. This will keep them on guard and ready to prevent a

cyberattack. We recommend users participate in simulated phishing tests weekly or biweekly. At a minimum, you should phish test users once a month. Phish testing users only quarterly or yearly provides a measurement; but phish testing users as often as possible shapes behavior.

A comprehensive security awareness plan should test users with multiple attack vectors, simulating real-life scenarios that they may encounter at work and at home. Simulating these attacks, prepares users with the knowledge they need to prevent a successful cyberattack on your organization.

4. Compliance

Based on the findings of the security risk assessment, Mosaic customers can see how they measure up to the standards set forth by the agencies who regulate their business. Mosaic provides compliance managed services for retailers, and any business that processes credit cards through scheduled compliance scans.

PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) applies to any organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. PCI is not, in itself, a law. The standard was created by the major card brands Visa, MasterCard, Discover, AMEX and JCB. At their acquirers'/service providers' discretion, merchants that do not comply with PCI DSS requirements may be subject to fines, card replacement costs, costly forensic audits, and brand damage, should a breach event occur. Merely using a third-party company does not exclude a merchant from PCI DSS compliance. It may lower their risk exposure and consequently reduce the effort to validate compliance, however it does not mean they can ignore the PCI DSS.

The Penalties for Non-compliance

The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks most often pass this fine along until it eventually hits the merchant. Furthermore, the bank will also most likely terminate their merchant relationship, or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business. It is important to be familiar with your merchant account agreement, which should outline your exposure.

Do Customers Processing Credit Cards Need Vulnerability Scanning to Validate Compliance?

If a merchant qualifies for certain Self-Assessment Questionnaires (SAQs), or electronically stores cardholder data post authorization, then a quarterly scan by a PCI SSC Approved Scanning Vendor (ASV) is required to maintain compliance. Mosaic provides ASV services. And, while scan results are required quarterly, we provide this scanning service on a monthly basis. By conducting monthly scans, Mosaic is able to have enough time to assist you with remediation. If you qualify for any of the following SAQs under version 3.x of the PCI DSS, then you are required to have a passing ASV scan:

- SAQ A-EP
- SAQ B-IP
- SAQ C
- SAQ D-Merchant
- SAQ D-Service Provider

What is a Vulnerability Scan?
A vulnerability scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool conducts a non-intrusive scan to remotely review networks and web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant, or service provider. The scan identifies vulnerabilities in operating systems, services and devices that could be used by hackers to target the company's private network. As provided by Mosaic ASV services, the scan does not require the merchant, or service provider, to install any software on their systems, and no denial-of-service attacks will be performed.

How Often are Businesses Required to Conduct a Vulnerability Scan?
A scan must be conducted every 90 days, or once per quarter, for those who fit the above criteria, and a passing scan must be submitted. Merchants and service providers should submit compliance documentation confirming successful scan reports according to the timetable determined by their acquirer. Once again, scans must be conducted by a PCI SSC ASV. With a little upfront effort and expenditure to comply with the PCI DSS, Mosaic can greatly help reduce your risk of facing any unpleasant and costly non-compliance consequences.

Why are PCI Risk Assessments and Vulnerability Scans Important?
Risk assessments are vital to an organization's ongoing security. They can uncover systems and processes that are actively putting you (or your customers' data) in harm's way.

First, it's important to understand merchant compliance obligations. Under section 12.1 of the PCI DSS, which relates to their information security policy, the subsection relating to risk assessments reads:

"Establish, publish, maintain, and disseminate a security policy that… includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include, but are not limited to, OCTAVE, ISO 27005 and NIST SP 800-30)"

Not exactly specific, but in fairness, there is an official set of PCI DSS Risk Assessment Guidelines, which go into more detail. Don't fancy reading it all right now? Here is the gist. In basic terms, the guidelines suggest that we can conduct risk assessments in whatever way we see fit, so long as it identifies threats and vulnerabilities that could negatively impact the security of cardholder data. The Mosaic recommended method for addressing this is the vulnerability scan.

Again, it's not just about compliance. Earlier, we put forward the idea that the official requirements for PCI compliance are not the most important thing to consider. After all, we're talking about the merchant customers' data here, and particularly sensitive data, at that. Any loss, or mismanagement of payment data, is going to have significant and long-lasting consequences, so it doesn't take much of a leap to conclude that conducting a risk assessment is a good idea.

With that in mind, the recommended steps go beyond simply identifying a few areas of concern, so we can prove we've done our due diligence, and then move into the realm of proactive data security. On a monthly basis, Mosaic will automate the vulnerability scans to occur on a predetermined basis.

Security Risk Assessment Follow Up
In the context of the PCI DSS, hackers are the most obvious potential threat actors. For the security risk assessment to maximize its effectiveness, it's essential that we fully examine all possible actors.

At this point, we have the scan results, so we can start to identify threats.

Threat Hunting - Some threats, such as asset vulnerabilities, are fairly easy to identify. As a starting point, we simply take the results of the last vulnerability scan, and subtract any that have already been remediated. But other threats will take much more thought. For instance, are there any elements in the merchant's processes that could potentially be exploited? If there are, this constitutes a real and measurable threat to their organization. How about your key personnel? They probably have privileged access to your network, so if your account were to become compromised, it could have serious consequences. This is where Mosaic Professional Services come into play. Our approach to addressing potential cyber threats is simplicity. Here is our methodology:

1. For every person, process, or asset involved in the assessment, consider what could potentially go wrong.
2. We then conduct an analysis of potential threats. It's not enough to simply know a threat exists.
3. Once we have a full list of threats, we make three calculations:

    Probability – The likelihood that a threat will actually occur

    Impact – The potential damage to your organization if a threat occurs

    Risk score – How dangerous a threat is, based on its probability and impact

There are literally hundreds of different processes for measuring these variables. Our method is to simply rank each risk on a scale of 1-4 for both probability and impact, and then take an average of the two to arrive at your risk score. For example, if a threat has a probability of 4 (very likely) and a potential impact of 2 (moderate), the risk score would be the average of those two figures - 3. Alternatively, if a threat is very likely (4) and potentially catastrophic (4), your risk score would be 4. These scores are important because they determine the order in which we prioritize risks for remediation.

Action: The Most Important Step

As with any vulnerability management, unless you actually act upon the results of the PCI DSS scan and risk assessment, there's really no point. Sure, it's a PCI requirement, but if you are only paying it lip service, it's only a matter of time before something goes seriously wrong. And at that point, compliance is going to be the least of your worries. That's why the most important thing to remember about conducting PCI scan engagements, is that it is a two-step approach with:

- Step 1 being the scan
- Step 2 analyzing the results of the scan, and remediating the issues

Once we have a prioritized list of threats, it's time to plan the remediation phase. Of course, there are some threats that cannot be nullified. Even if they have a risk score of 4, we're just going to have to accept them. On the other end of the scale, some low risk threats can be accepted for now to keep resources free for more important remediation work. Mosaic will make sure you are aware of them, and have the proper steps in place to deal with the damage, if they do become a reality.

For other threats, Mosaic Professional Services will determine the best course of action… and then do it. It will require time, effort, and resources, but this is what the whole risk assessment process is about. Mosaic simplifies this entire process, ensuring your customers' payment data is safe and secure.

5. Managed Threat Intelligence Including Incidence Response

The ever-increasing number of cyberattacks, security breaches, and mounting regulatory requirements, are straining IT departments, particularly for small and medium sized organizations with limited in-house IT budgets
and personnel.

Organizations that lack technical controls, procedures and financial resources required to develop, staff and operate viable threat-monitoring and breach detection capabilities in-house, are vulnerable to cyberattacks.

To overcome this problem, the Mosaic managed threat intelligence service provides premium actionable threat intelligence at an affordable price. Mosaic managed services for Security Information and Event Management (SIEM) leverages our network and security operations center (NOC/SOC) to provide event management and remediation guidance. Layered within our NOC/SOC platform are monitoring dashboards that depict the status of events (low, medium, and high) to proactively alert customers and remediation parties of threats.

A key focus is to monitor and help manage user and service privileges, directory services and other system-configuration changes; as well as providing log auditing and review, and incident response. As a SIEM, our NOC/SOC has visibility into our customers' LANs, WANs, and SaaS applications, receives alerts to potential attacks or anomalies, and proactively alerts customers, while performing remediation.

Mosaic Managed Threat Intelligence Service (MTIS) provides up-to-date cybersecurity threat alerts and the remediation guidance needed to deflect them. Our MTIS actively monitors your networks for possible hacking attempts and intrusions into your systems. The service provides you with all hardware, software, and sensors needed to analyze and monitor threats affecting your network. Mosaic works directly with you to ensure the implementation and completion of all recommended patches and fixes.

Mosaic Managed Threat Intelligence as-a-Service Details

Deployment	• Inventory scanning and asset registration • Network and endpoint monitoring • Baseline vulnerability environment scanning • Event zcorrelation, tuning and alarm trimming • Basic threat dashboard and report creation
Alarm Monitoring	• 24x7 SOC Coverage for Severity Level 1 • 12x5 SOC Coverage for Severity Levels 2 • 9x5 SOC Coverage for Severity Levels 3-4
SIEM Tuning	• Continuous
Ticket Creation	• Included
Threat Analysis	• 24x7 SOC Coverage for Severity Level 1 • 12x5 SOC Coverage for Severity Levels 2 • 9x5 SOC Coverage for Severity Levels 3-4
Remediation Guidance	• Included
Service Review	• Monthly SIEM and SOC Service Review
Client Portal Access	• High level threat intelligence dashboard (trending, security KPIs) • Ticket management and reporting (support, alarms, incidents, and change) • Industry feeds and advisories • Monthly readouts and compliance reports • 3 portal accounts come standard
Threat Management™ Console Access	• Read-only Appliance access • Inventory and asset management • Network and endpoint management • Environmental scanning and vulnerability management • Alarm management, ticketing, change management, and forensics capabilities to evaluate events • Basic threat intelligence reports
Lifecycle Management	• Platform updates, signature updates, platform maintenance • Verification of data backup; configuration and job status • Health monitoring of service software and appliances

The Mosaic NOC/SOC performs these activities so your network can be monitored, and customized rules can be created for event correlation to trigger alerts. These are based on certain conditions from various log sources, such as network devices, security devices, servers and antivirus. These customized rules for event condition alerts can involve user authentication, attacks detected, and infections detected. Thresholds can be configured to trigger alerts based on the quantity of occurrences.

Additionally, a PR response plan is one of the most overlooked aspects of a holistic incident response program. Depending on your type of business, you must be prepared to quickly react to breaches, by truthfully and accurately notifying employees, customers, business partners, and possibly the government and media.

A thoughtful crafting of these announcements and setting up a response platform to distribute them in a timely manner is essential. While Mosaic does not offer this service, as a trusted advisor we recommend that our customers engage professional corporate communications specialists and/or public relations experts to assist in the crafting of responses tailored for your business. These responses should be reviewed and possibly modified over time.

Cybersecurity Protection Involves an On-going Program

Understanding security requires a keen awareness of the ever-changing risk factors. Overcoming these risks requires communication, planning, training, testing and remediation. Ensuring successful cybersecurity protection also involves an on-going program. As the threat vector landscape is always changing, it's important to protect your organization against the latest threats.

Most businesses spend the majority of their time and effort optimizing profits and growing the business. These are the typical measures by which they judge success. Yet, the lack of a cybersecurity program can quickly undo a successful company. Security breaches pose many risks, including lost revenue, legal liability, loss of brand equity and customer trust.

To minimize the threat of security incidents and breaches, enterprises must have a proper cybersecurity program is in place. This will enable business and IT leaders to create a robust, reliable, and trusted infrastructure in which to operate safely and securely.

Cyberattacks use many different techniques to evade detection. To thwart these attacks, and stay ahead of the attackers, enterprises must have effective security measures. This includes properly trained people, effective processes and deployment of security technologies, with best practices implemented throughout.

Albert Einstein famously said, "the definition of genius is taking the complex and making it simple." Every year, enterprises get more complicated, with myriad network connected devices, increasing numbers of mobile workers, a growing number of cloud and SaaS applications, and much more.

It's easy to make things complicated. The difficulty is making them simple. Mosaic's managed cybersecurity services take the complexity and burden away from our customers, allowing them to focus on their core competencies, and grow their business.

Mosaic NetworX Managed Security Services

Cyber Security is a concern of all businesses, and Mosaic NetworX provides cyber security tools, methodologies, and expertise to assist business in meeting the goal of becoming cyber resilient. We work with SMB and mid-market businesses to provide them with the same tools and methods that large enterprises use to achieve that end. Cybercriminals know smaller organizations have fewer resources to dedicate to data security, making them an easier target. Compromising just one user often grants the "keys to the castle." Put another way, just one simple click on an infected email or malicious link and the entire company is in trouble.

Many SMB and mid-market businesses are faced with the fact that it's nearly impossible for an internal IT staff that's probably already overtaxed to keep up with the dozens of threats to that come in every day, no matter what tools they're using. Tools, by themselves, won't secure the business either. Real security requires discipline, an overarching methodology and sufficient resources. Mosaic NetworX brings the discipline, methodologies, and resources necessary to secure the network, assets and employees.

To learn more about the Mosaic cybersecurity managed services, contact us at info@mosaicnetworx.com.