CYBERSECURITY

Presented by: PSA SECURITY NETWORK

PLAYBOOK SERIES

PLAYBOOK ONE
TIER ZERO

FOREWORD

It has been said that a rising tide floats all boats. It is the goal of our PSA cyber security committee to raise the qualitative and quantitative cyber assurance capacities of every PSA Security Network owner/member that engages with us in this effort. This playbook series is the tide that will raise our organizations to higher ground, towards *a higher level of maturity* in cyber security framework jargon.

This is not a simple undertaking, but it is also not a mystery. Much guidance is already provided and spelled out through government and commercial undertakings involving untold hours of think-tank level brain power conducted over the last decade or so. The **great** news is we don't have to reinvent the wheel. More great news; this committee has distilled thousands of pages of guidance into step-by-step playbooks that you can follow to achieve an ever higher level of cyber security maturity for your organization, people, in your processes, and in your products/systems. The **bad** news; you have a tough decision to make: "When should I start and will we see it to the end?"

As executives, owners, CEOs, management, etc., you have a fiduciary responsibility to protect your company, its shareholders, employees and customers. This responsibility includes detecting risks the organization and mitigating those risks. Ignoring risks, any risk, to include cyber risk, may be considered negligent and create liability. Pushing the risk and mitigation responsibility off to a vendor, supplier, the IT department or other is not a solution, and equally claiming it is a technical problem so not your issue is not a solution either. To protect your organization, you must take a proactive and comprehensive approach to this new and quickly increasing risk. As the leader you are responsible and we are here to help you.

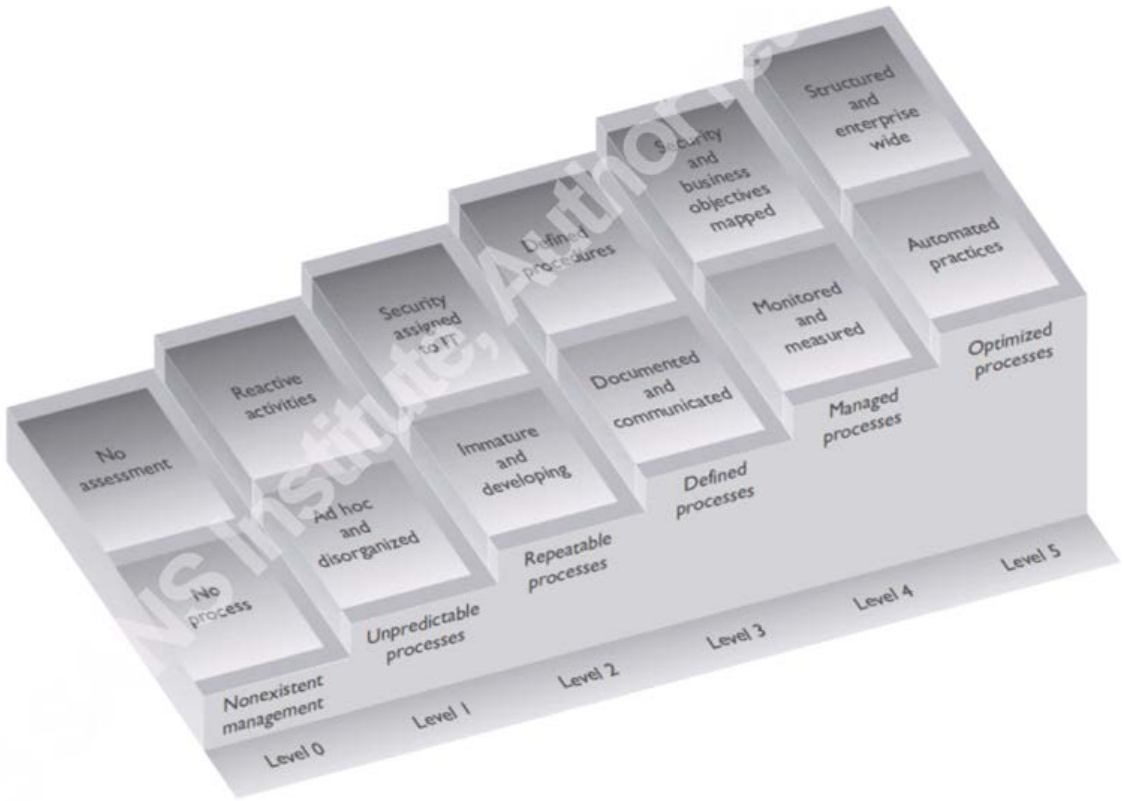
This committee believes we are all behind the power curve and therefore should start immediately. This playbook series consists of five Tiers, Tier Zero through Tier Four. Each designed to move you progressively closer to better cyber and information security. Each Tier consists of a series of brief Yes or No questions that you will be able to answer in a couple of minutes or less. Tier Zero is the starting point. Once you have completed the Tier Zero questions, you can review your answers against our prepared responses which will help you determine your follow-on steps. One caution, the goal is not to cause you stress. Your score is a gauge for you. We are all in the same boat and this is new to most of us. Our desire is to embark on this journey, and learn and become more cyber secure together, for our businesses, clients and industry.

See you on dry ground ~

Andrew Lanning, Chairman, PSA Cyber Security Committee

This cyber security playbook is a maturation tool. It is deployed for use by PSA owner/member organizations to mature their internal and external cyber security people, process, and products. We've borrowed the word *mature* from the CMMI community (Capability Maturity Model Integration). It is one way of describing the evolution of people and processes within a given framework. An example "process guidance" model is included below in Picture 1. Notice that at each level the activities and documentation associated with this model's organizational processes increase in breadth and detail, thus indicating the *maturity* at each level.

Picture 1



The reason we chose CMMI for this playbook is that it adapts readily for understanding organizational maturity within the NIST (National Institute of Standards and Technology) Cybersecurity Framework.

The NIST Cybersecurity Framework has a *Core* element which is the functional basis of the activities that describe an organization's life cycle of risk management. The second element of the framework is the *Implementation Tiers* which reflect an organization's current level of maturity compared to the characteristics within the framework. The final element is the *Profiles* which define where an organization is (current profile) in comparison to where it wants to be (target profile) for any particular cyber security characteristic of the organization.

The left hand column of Picture 2 below shows the five functional activities at the core of the NIST Cybersecurity framework: Identify, Protect, Detect, Respond, and Recover.

Picture 2

ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Notice how each section is divided into subsections as you move to the right. In turn, each of these subsections has components that can be mapped to 1 or more "security controls." That's how the 5 simple ideas on the left become hundreds of controls in the real world. There is additional reference information in the Resource Guide of this playbook series if you want to learn more about the NIST Cybersecurity Framework, the SANS top 20 controls, or the Center for Internet Security Controls Version 6.

Our suggestion is to take the Tier Zero test in the next section, then pick one item a week and work on it within your organization until you can answer yes to all Tier Zero questions. That work alone will teach you about framework outcomes, which from a near-term practical perspective is more valuable than understanding the framework itself.

Following the questionnaire you will see a variety of mitigation responses, or advice, for each Yes and No question and answer response. Once your organization can answer yes to all the items in the Tier Zero questionnaire portion, then you will be ready to move on to the Tier One questionnaire and so on and so forth. We're confident that if you use this playbook, your organization will grow towards a cyber security maturity level that meets with your industry and your client's requirements. As your boat rises so will all PSA Security Network boats rise.

Starting at Tier Zero allows your organization to explore it's current state of cyber awareness and build from the ground up! You should be able to answer the following questions relatively quickly and with confidence. Questions you can't answer should be scored as a NO. Now, just to be clear, these questions should be answered by you, the leadership, first. Then, once completed, speak with your technical team to find out how accurate you were. If you got some or many wrong, having put a No when the answer should have been Yes, then you are better off than you thought you were; bonus! Changing questionnaire NO's to YES's is the goal, that's a good thing.

Anticipate that as your organization moves to higher levels of cyber security maturity that you will need to consult with higher level technical resources, both inside and outside of your organization. Eventually you will need third party auditors to help assess what your team is accomplishing. These are good goals to achieve in the cyber security world, so embrace them as they come to you and count yourself among the fortunate who are engaged enough to understand the necessity. Now, let's get on with your TIER ZERO assessment.

People Section Questions **Answers**

Have you conducted cyber awareness or information security training with your staff in the past 3-6 months? (NIST 800-53 rev 4) Awareness Training (AT-2) Yes No

Have you conducted anti-phishing or social engineering training with your staff in the past 3-6 months? (NIST 800-53 rev 4) Awareness Training (AT-4) Yes No

Do you have any cyber security experts on your staff?
(NIST 800-53 rev 4) Awareness Training (AT-3) Yes No

Is your staff aware of their cyber threat exposure when opening email attachments or browsing the internet? (NIST 800-53 rev 4) Incident Response (IR-7) Yes No

 # Yes - _____/4

Processes Section Questions **Answers**

Does your company perform daily backups?
(NIST 800-53 rev 4) Contingency Planning (CP-9) Yes No

Does your company retain Personally Identifiable Information (PII) client system information (drawings, network schemas, etc.) on your network?
(NIST 800-53 rev 4) Access Control (AC-21) Yes No

Does your company use data encryption for internal information?
(NIST 800-53 rev 4) Systems Communication (SC-33) Yes No

Is your network scanned for vulnerabilities on a periodic basis?
(NIST 800-53 rev 4) Systems Integrity (SI-3) Yes No

Does your company have a cyber insurance policy?
(NIST 800-53 rev 4) Program Management (PM-9) Yes No

Does your company have an information security policy?
(NIST 800-53 rev 4) Program Management (PM-1) Yes No

 # Yes - _____/6

Products Section Questions	Answers
Does your company use a password management system? (NIST 800-53 rev 4) Information Assurance (IA-5)	Yes No
Does your company use a firewall or network monitoring tool? (NIST 800-53 rev 4) Systems Communication (SC-28)	Yes No
Does your company use a mobile device management system? (NIST 800-53 rev 4) Access Control (AC-19)	Yes No
Does your company maintain a log of all attached network equipment and firmware versions? (NIST 800-53 rev 4) Configuration Management (CM-8)	Yes No
Does your company use a multi-factor authentication physical access control system for premises entry? (NIST 800-53 rev 4) Information Assurance (IA-5)	Yes No
Does your company use a multi-factor authentication login for access to network resources? (NIST 800-53 rev 4) Information Assurance (IA-5)	Yes No

 # Yes - _____/6

Tier Zero Total (People + Processes + Products)

 # Yes - _____/16

Q1: Have you conducted cyber awareness or information security training with your staff in the past 3-6 months?

Yes Response Next Steps

1. Test your team on the past training to ensure current comprehension levels, log your results
2. Schedule complete annual cyber awareness training on an annual basis, log results
3. Schedule bi weekly or monthly game or email updates to maintain staff awareness, log results

No Response Mitigations

1. Schedule Employee Cyber Security Awareness Training Immediately, log results
    a. UDEMY Cyber Security: Build a Secure Resilient Company https://www.udemy.com/confidentdefensefoundation/

2. Schedule Employee Information Security Training Annually, log results
    a. SANS https://securingthehuman.sans.org/security-awareness-training/overview
    b. MICROSOFT (Do it yourself download materials) https://www.microsoft.com/en-us/download/details.aspx?id=10484

3. Setup a Continuous Employee Security Awareness Training Program, log results
    a. MICROSOFT (Do it yourself download materials)https://www.microsoft.com/en-us/download/details.aspx?id=10484
    b. SANS (Presentations and Planning Kit) https://securingthehuman.sans.org/resources/planning

4. Not Confident doing this internally?
    a. Speak with experts from the PSA Vendor List in the Resource Guide

Q2. Have you conducted anti-phishing or social engineering training for your staff in the past 3-6 months?

Yes Response Next Steps

1. Test your team on the past training to ensure current comprehension levels, log results
2. Schedule complete annual cyber awareness training on an annual basis, log results
3. Conduct monthly active spear-phishing test campaign to test staff competency, log results

No Response Mitigations

1. Schedule Employee Phishing Training Immediately, log results:
    a. Cybrary: Social Engineering & Manipulation (Free) https://www.cybrary.it/course/social-engineering/
    b. UDEMY Cyber Security For Beginners. Avoid Business Data Breaches: https://www.udemy.com/cyber-security-for-beginners-avoid-business-data-breaches/

2. Distribute, Review, and Post SANS "Don't Get Hooked" poster:
    a. https://securingthehuman.sans.org/media/resources/STH-Poster-DontGetHooked.zip

3. Administer this course from UDEMY, Mobile Cyber Security Awareness, log results:
    a. https://www.udemy.com/mobile-security-awareness-training/

4. Not Confident doing this internally?
    a. Speak with experts from the PSA Vendor List in the Resource Guide

Q3. Do you have any cyber security experts on your staff?

Yes Response Next Steps

1. Verify Staff Security Certifications are current
2. Plan & Budget for annual certification updates and upgrades
3. Have staff create and manage company Information and Cyber Security Policies
4. Make Off-boarding plans to minimize intellectual property leakage

No Response Mitigations

1. Training internal staff. See Education and Training Resources: Chapter 11
    a. CIS Cybersecurity Workforce Handbook https://www.cisecurity.org/workforce/images/Workforce.pdf

2. Hire Certified Professional
    a. Monster.com search for cyber security (1000+) http://jobs.monster.com/search/?q=cyber-security
    b. CareerBuilder.com search for cyber security (1600+) http://www.careerbuilder.com/jobs/keyword/cyber-security
    c. Indeed.com search fro cyber security (15,000+) http://www.indeed.com/q-Cyber-Security-jobs.html

3. Conduct cyber risk assessment to determine hiring requirements.
    a. Speak with experts from the PSA Vendor List in the Resource Guide

Q4. Is your staff aware of their cyber threat exposure when they open email attachments or browse the internet?

Yes Response Next Steps

1. Test your team on the past training to ensure current comprehension levels, log results
2. Conduct Active Phishing campaign to test your staff awareness levels, log results
3. Implement a periodic phishing campaign to maintain staff awareness levels, log results

No Response Mitigations

1. Schedule Employee Phishing Training Immediately:
    a. UDEMY Cyber Security For Beginners. Avoid Business Data Breaches: https://www.udemy.com/cyber-security-for-beginners-avoid-business-data-breaches/

2. Distribute, Review, and Post SANS "Don't Get Hooked" poster:
    a. https://securingthehuman.sans.org/media/resources/STH-Poster-DontGetHooked.zip

3. Administer this course from UDEMY, Mobile Cyber Security Awareness:
    a. https://www.udemy.com/mobile-security-awareness-training/

Q1. Does your company perform daily backups?

Yes Response Next Steps

1. Are full backups completed at least daily?
2. Are backups stored off site?
3. Do you test restoring your backups on a regular basis?

No Response Mitigations

1. Begin backing up immediately.
2. Speak with experts from the PSA Vendor List in the Resource Guide

Q2. Does your company retain Personally Identifiable Information (PII) or client system information (drawings, network schemas, etc.) on your network?

Yes Response Next Steps

1. Are these items being stored on laptops, server, or sharepoint site?
2. Do you have a policy that addresses PII that all employees must sign and acknowledge?
3. Are your technicians allowed to copy data from client sites?
4. Seek guidance from the PSA vendor list for a complete understanding of all existing storage of PII.

No Response Mitigations

1. Obtain policy that is inclusive of handling sensitive data
2. Create ongoing awareness program.
3. Speak with experts from the PSA Vendor List in the Resource Guide

Q3. Does your company use data encryption for internal information?

Yes Response Next Steps

1. Is full disk encryption utilized on every machine?
2. Have you performed a data classification exercise for information stored on your network?

No Response Mitigations

1. At a minimum, you should have full disk encryption deployed on technicians in the field as well as your HR and Financial resources
2. Speak with experts from the PSA Vendor List in the Resource Guide

Q4. Is your network scanned for vulnerabilities on a periodic basis?

Yes Response Next Steps

1. Add active 3rd party monitoring where possible.
2. Conduct 3rd party external audits to confirm internal audit findings.
3. Ensure report logs correlate events over time properly.
4. Conduct and log 3rd party penetration tests on a regular basis. Consider varying vendors for the PEN testing and Vulnerability analysis.

No Response Mitigations

1. Document network vulnerabilities immediately, log results.
    a. https://nmap.org/
2. Seek guidance from the PSA Vendor list to establish the process.
3. Have a third party audit the results on a regular basis, log findings.

Q5. Does your company have a cyber insurance policy?

Yes Response Next Steps

1. Is your policy reviewed annually to determine the right coverage?
2. Have you reviewed client contracts to determine if your coverage is aligned?

No Response Mitigations

1. Speak with experts from the PSA Vendor List in the Resource Guide

Q6. Does your company have an information security policy?

Yes Response Next Steps

1. Schedule annual policy reviews
2. Check for missing Policy Elements
    a. Infosec Institute http://resources.infosecinstitute.com/key-elements-information-security-policy/
    b. SANS Development Guide https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331
    c. GIAC Elements of Security Policy – Considerations for Small Businesses https://www.giac.org/paper/gsec/3495/elements-security-policy-considerations-small-businesses/102691
3. Speak with experts from the PSA Vendor List in the Resource Guide

No Response Mitigations

1. Create an Information Security Policy
    a. Outsource(s)
        i. Speak with experts from the PSA Vendor List in Chapter 12
    b. Research for internal creation (IT Staff required)
        i. SANS Information Security Policy Templates https://www.sans.org/security-resources/policies/
        ii. SANS Security Policy Roadmap https://www.sans.org/reading-room/whitepapers/policyissues/security-policy-roadmap-process-creating-security-policies-494
        iii. Center for Internet Security Cyber Security Guides https://msisac.cisecurity.org/guidelines/index.cfm
        iv.
    c. Internal Creation (IT Manager Required)
        i. Refer to all Yes/No response documents in this Next Step/Mitigation Answer

Q1. Does your company use a password management system?

Yes Response Next Steps

1. Does the password policy forbid the reuse of passwords and generate automated and secure passwords for the users? (Typically many characters, symbols, numbers)
2. Do you encrypt your computer's hard drive? Web based browsers store passwords in an unencrypted format on the computer, and is potentially vulnerable to attack.
3. Does the password management system protect mobile devices with two-factor authentication?

No Response Mitigations

1. Many companies provide device and browser support, as well as multi-factor authentication: 1Password (www.agilebits.com), DashLane (www.dashlane.com), LastPass (www.lastpass.com), Roboform (www.roboform.com), & Stickypassword (www.stickypassword.com).
2. A variety of software programs exist to encrypt hard drives. Resources to consider include the following sites: Bitlocker, (www.exo5.com/full-disk-encryption) for Windows, and FileVault 2 (www.support.apple.com) for Mac.
3. The future of password technology includes multifactor biometrics: facial and photo recognition, keystroke pattern recognition, fingerprints, etc., in addition to geo-location services and traditional password inputs to allow for secure cross platform access.

Q2. Does your company use a firewall or network monitoring tool?

Yes Response Next Steps

1. Do your network tools provide visibility into any additional devices (network servers / storage / mobile platforms) and users that might be added to your network? Can you identify power usage, anomalous behavior, and remote access?
2. Do you utilize a security command center platform to update and manage your firewall and related cyber threat intelligence services?
3. Have you written Service Level Agreement (SLA) verbiage into vendor and third party contracts to detail security policy and assure specific uptime requirements?

No Response Mitigations

1. Various vendor solutions exist to provide information on network asset inventory (operating systems, software, etc.), traffic pattern analysis, identity & access control, log management, intrusion detection, Security Information & Event Management (SIEM), etc. It is important to keep these devices updated and also understand how failure (component / systemic) will impact your business operations.
2. With network configurations and cyber threats constantly changing, a centralized approach to security management is an imperative. Timely updates of software releases, malware patching, and near real time threat intelligence feeds, must all integrate seamlessly if you are to provide the best response to internal and external attacks. Most cyber security vendors will provide a central platform to incorporate these policies and include real time reputation based filtering for firewalls.
3. Contracts should involve an understanding of, and visibility into, how your data is stored / accessed, and transmitted and by whom. Third party contractors, vendors, and outsourcing providers should have policies for vetting employees and securing systems. All supply chain partners, vendors, or outsourced providers should detail security procedures and explain in writing best efforts to protect your information and company reputation against potential breaches.

Q3. Does your company use a mobile device management system?

Yes Response Next Steps

1. Is there a policy that is included in the Information Security handbook that outlines that company information collected or stored on mobile devices is the property of the company?
2. Does the policy extend beyond mobile phones and cover ipads, tablets, and other smart devices (i.e. watches)?
3. Have you tested the device for security, encryption and data wiping?

No Response Mitigations

1. Retain the services of a qualified consultant or team member to identify company essential services that are provided to employees via mobile devices.
2. Isolate or eliminate unnecessary services that are provided over mobile devices to employees that are not needed.
3. Select and deploy an appropriate MDM Solution.

Q4. Does your company maintain a log of all attached network equipment and firmware versions?

Yes Response Next Steps

1. Conduct a periodic review to insure that the log of all attached network equipment and firmware versions are documented and kept offsite in a secure manner.
2. Identify and compare changes to diagrams and documentation to ensure they are up to date
3. Use asset tags to correlate devices to network equipment to inventory

No Response Mitigations

1. Use electronic and manual procedures to capture network equipment (100% accuracy required)
2. Visually document equipment and location., owner, and diagram if possible
3. Create and maintain a log of all attached network equipment and firmware versions.

Q5. Does your company use a multi-factor authentication physical access control system for premises entry?

Yes Response Next Steps

1. Confirm deployment is aligned with company policies on use of authentication.
2. Confirm company established security controls are implemented in the physical security system.
3. Confirm enterprise infrastructure management standards (maintenance, documentation) are in place.

No Response Mitigations

1. Evaluate whether you are using sufficiently strong authentication for the area under physical access control.
2. Identify areas that should be under stronger access control.
3. Incorporate biometrics, keypads, etc. into your access control.

Q6. Does your company use a multi-factor authentication login for access to network resources?

Yes Response Next Steps

4. Confirm deployment is aligned with company policies on use of authentication.
5. Confirm company established security controls are implemented in the physical security system.
6. Confirm enterprise infrastructure management standards (maintenance, documentation) are in place.

No Response Mitigations

4. Evaluate whether you are using sufficiently strong authentication for the area under network access control.
5. Identify areas that should be under stronger access control.
6. Incorporate biometrics, keypads, etc. into your access control.