PSA committee CYBERSECURITY

Risks Involved With A Cyber Incident

Operational Risk

- Operations & Technologies shut down and are unable to be used so employees cannot produce.
- Comfort, automation & health safety systems controlled by network become inoperable.
- Internal & external email and telephones are often shut down.
- Ecommerce & banking systems are shutdown or heavily impacted.
- Public facing websites are often taken down or unusable.
- Physical security infrastructure operations & communications are often affected.

Financial Risk

- Loss of productivity & revenues add up quickly when employees cannot work.
- Bank and payment processing systems are often affected, severely limited, and made unusable. Making payments or bringing money in from sales impossible.
- Paying ransomware is often expensive and does not guarantee your data back. Deals made with criminals often do not pay off.
- Cost to recover your data and restore your IT systems are often excessive and the work is time consuming.

Legal Risk

- Failure of notification services of the breach by city, county, state & country as required by the entities & within the required timeline may result in large fines.
- Potential litigation with customers & vendors.
- Potential criminal suit brought against the company and executives.
- Potential civil lawsuits from those that you have exposed PII, PHI & other personal data.

Reputational Risk

- Your brand can be irrevocably hurt by a cyber attack.
- Those you serve may lose trust in your ability to conduct business.
- High-profile dealings with law enforcement after a breach are often publicized by the media.
- The method and timing of notifying the media and others about the breach may provide severe backlash on the company and leadership.

For More Information on Reducing Your Risk

- Reference CIS Controls – Organization Sections 17, 19, 20

PSA committee
CYBERSECURITY

Identify and Understand Cyber Threat Actors and Typical Methods of Attack

Organized Crime

The primary threat for most SMB, commercial and government entities is by criminals looking to make money! With Crimeware-as-a-service (CaaS), organized crime is franchising cybercriminal underlings with tookits, resources and hosting services. The risk associated with conducting cybercrime is dramatically imbalanced relative to the reward in favor of these criminals as very few are identified, apprehended and prosecuted.

Motivation: Financial gain or reputational enhancement
Affiliation: Individuals or with collaborators
Common Tactics, Techniques and Procedures (TTPs): Phishing, social engineering, business email compromise (BEC) scams, botnets, password attacks, exploit kits, malware, ransomware

Nation States - Advanced Persistent Threat (APT) Groups:

Threat Actors have evolved over the last decade. The most significant threat to the world is the Nation State / APT Threat Actor. These Cybercriminals are highly organized and have unlimited funding and resources. The disparity of threat versus defense against the Nation State is so extreme it is almost immesurable.

- Russia 52%
- Iran 25%
- China 12%
- North Korea and other countries 11%

j

Motivation: Espionage, political, economic or military
Affiliation: Nation-states or organizations with nation-state ties
Common TPPs: Spear-phishing password attacks, social engineering, direct compromise, data exfiltration, remote access trojans and destructive malware

Insider Threat

Those under your company employ or contract that exfiltrate precious or sensitive information out of the company for nefarious objectives. Insiders undermine cybersecurity and physical security because they often have legitimate access to data and can carry out their criminal intent while appearing to conduct normal work activity.

Motivation: Financial gain or to seek revenge
Affiliation: Current or former employee, contractor, or other partner who has authorized access
Common TPPs: Data exfiltration or privilege misuse

Hacktivists

A.k.a. ideologically-motivated criminal hackers, target high-profile entities/ victims to garner notoriety and publicity and to make political or social statements, often in an effort to affect change.

Motivation: Political, social or ideological
Affiliation: Non-governmental individuals or organizations
Common TPPs: DDoS attacks, doxing, website defacements

Terrorist Organization

These groups are designated by the U.S. Department of State. Their cybercrime is typically disruptive and or harassing in nature.

Motivation: Political or ideological; possibly for financial gain, espionage, or as propaganda
Affiliation: Individuals, organization, or nation-states
Common TPPs: Defacements and claimed leaks

For More Information on Reducing Your Risk:

- Reference PSA CIS Controls Whitepaper
- CIS Controls - Organizational Control 17

Resources: Microsoft; Center for Internet Security (CIS)

PSA committee CYBERSECURITY

Creating Cyber Security Leadership and Culture

Building a Top-Down Culture

Executive Support, Participation & Knowledge

- Buy-in and support from Senior Leadership is the crucial first step to the success in building a Cyber Security Culture in your organization.
- Participation and knowledge are what sustains it.

Clear Communication Plan

- Communication can make or break the plan.
- Provide good communication early and often to keep your employees informed and engaged.
- Share successes.

Awareness Education & Training

- Remember, your employees are not Cyber Security Experts. They are good at doing the things that make your organization run.
- Invest in good tools to educate them and make it fun!

User Friendly Process/ Tools

- Ease of use goes a long way in adoption of the Cyber Security Culture.
- If it's difficult and time consuming, employees are likely to go around it.

Celebrate the Wins & Don't Promote Shame

- Remember you are starting from zero.
- When something good happens, celebrate it!
- When a mistake is made, learn from it.

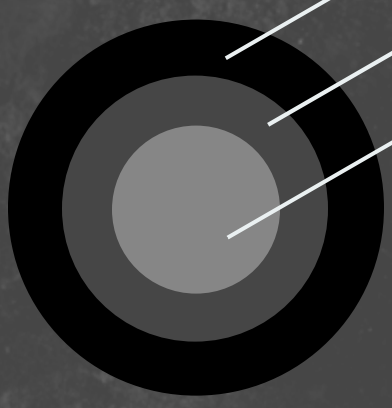
Performance Evaluation

- Evaluation starts at the top. Participation and awareness are needed at every level of the organization.
- Be honest about how your organization is performing.

Culture Transformation

- The goal is to sustain transformation.
- This isn't a project it is a culture shift.

How Roles Are Dispersed in Different Sized Organizations



Large - Roles are typically separated out to departments for each area

Medium - Roles fall under 2-4 employees

Small - All roles under one/ two employees

Roles

- Executive Sponsor
- Communications
- Policy Maker
- Procedure Writer
- Implementation
- Monitoring/Maintaining

References
https://www.cisecurity.org/?s=CIS+RAM
https://cams.mit.edu/wp-content/uploads/Building-a-Culture-of-Cybersecurity.pdf
https://www.cira.ca/blog/cybersecurity/what-cybersecurity-culture-and-how-do-you-build-it

PSA committee CYBERSECURITY

Employee Awareness and Social Engineering

Bringing Awareness

Assess Employees - Skills Analysis

- Perform a skills analysis to understand workforce members' skills and behaviors.
- Know areas they are weak in or not adhering to.

Change Behavior - Create a Security Awareness Program

- Learning Media and Reminders
  - Such as internal newsletters or posters in the lunchroom.
- Phishing Awareness Campaigns
  - Employees are baited with phishing emails by their employer to help educate them on how to spot and report actual phishing attempts. This helps protect themselves and the company.
- Automated Online Training & Classroom Training
  - The training in specific, tailored and focused based on the specific behaviors and skills needed by the workforce, depending on an employees job role and responsibility.
- Vendor/ Product Tools for Cyber Education
- Create a Security Awareness Program
  - Every employee understands their role to ensure the security of the company.
  - Spell out obligations and expectations.

Track Metrics & Update Training

- Training is repeated periodically, measured and tested for effectiveness and updated regularly.

Social Engineering Threats

Phishing

The fraudulent practice of sending emails or other electronic communications, appearing to be from reputable sources to trick individuals into revealing private information.

- Spear Phishing
  - Targets a specific group or type of individuals, such as a company's Accounting Department
- Whaling
  - An even more targeted attack usually aimed at Senior Executives within an industry or business.
- Smishing
  - An attack that uses text messaging for SMS to fraudulently send a message to your cell phone to entice you to click on a link or call a phone number.
- Vishing
  - This is an attack involving voice calls with either a conventional phone system, cell phone, or Voice over Internet Protocols (VoIP) systems.

Default or Common Passwords

- Default Passwords
  - Many internet-connected devices, such as routers and webcams, initially come with default usernames and passwords to allow new users to log into and configure them easily. Many people neglect the important step of changing or removing the default login information, leaving them vulnerable to attack.
- Common Password
  - This is when someone uses a very simple (common) password like "password" or "secret" Choosing common passwords makes it easier for an attacker to gain access.

Clicking URL's

- A malicious URL is a link created to promote scams and attacks. By clicking on an infected URL you can download malware onto your device, or you can be persuaded to provide sensitive information.

Public WiFi

- The same features that make public WiFi desirable to consumers also make them desirable for cybercriminals. They require no authentication to establish a network connection, which makes you vulnerable.

USB Drives

- Can pose a severe security risk to networks and data. USB drives can be used to transmit malware. Don't ever plug in a USB drive that's not yours or that you don't trust. If your USB drive is not encrypted attackers may steal sensitive information. USB drives are easily lost or stolen, so back them up regularly.

Backup Data

Having valid data backups are the last line of defense against an attack.

- Ensure that all system data is automatically backed up on a regular basis.
- Test data integrity on backup media on a regular basis.
- Ensure that backups are properly protected via physical security or encryption when they are stored.
- Ensure that all backups have at least one offline backup destination.

PSA committee CYBERSECURITY

Assess the Vulnerabilities of Your Critical Business Systems, Data and Network

Contrary to popular belief, a Vulnerability Assessment is not an Information Technology Function. Information Technology is not synonymous with Information Security. Information Technology personnel are responsible for the day-to-day operation and up time. It has often been said that the IT person has it covered. Do they really have it covered? Operational IT people live in the "Availability" world. If the system is up and functional then they are doing their jobs. As a rule, temporary, on the fly solutions tend to remain permanent and may introduce risk into your organization.

Information Security Professionals are a bit of a different breed. They have a completely different point of view. They live in the world of "Confidentiality" and "Integrity" while balancing "Availability". Information Security is really all about assessing and mitigating risk according to the risk appetite of the organization.

Your first Vulnerability Assessment provides a baseline and gives your organization an accurate snapshot of the current Cyber Security Maturity status. Vulnerability Assessments should be conducted at regular intervals because the threat landscape is constantly changing. These assessments are a key part of your organization's Cyber Security Posture.

An Assessment is Composed of Four Main Parts

Technical Component

Technical vulnerabilities are discovered by using automated vulnerability assessment tools such as Tenable Nessus, Rapid 7 and Greenbone Vulnerability Server for example. These scanners have the ability to discover thousands of confirmed, common vulnerabilities that are known to exist in Operating Systems, Applications, Server Software and Firmware. The commercial versions of these products also provide detailed technical reporting.

Some of these scanners are open source but a majority of them are commercial licensed software. The commercial versions of these scanners are usually sold by subscription and your organization will incur annual fees to maintain licensing and receive vulnerability updates.

In some cases, Manual technical assessments are used to examine systems for misconfiguration and less commonly known vulnerabilities. This is sometimes referred to as penetration testing. Penetration Testing methodology is designed to compromise the security of a system.

Control Assessment

Your risk assessment should be used as a guide to determine which Cyber Security Controls should be implemented. These controls should be outlined in the System Security Plan for each system that your organization is using. A Controls assessment confirms that the selected security controls are effective for the desired outcome.

Report

Your risk assessment should be used as a guide to determine which Cyber Security Controls should be implemented. These controls should be outlined in the System Security Plan for each system that your organization is using. A Controls assessment confirms that the selected security controls are effective for the desired outcome.

Remediation Plan with Actions and Milestones

A more technical report can be given to the Technology Leaders in the organization. This report should provide specific and granular information as to the vulnerabilities, severity and remediation steps required. A plan of actions and milestones should be drafted to ensure that mitigation efforts directed and maintain momentum.

A Vulnerability Assessment is a key component in your organization's overall Information Security Strategy. These assessments provide a view into your organization's critical business systems to identify and mitigate the associated risks. It is up to your management team to determine if you have the resources, both monetarily and talent, to effectively perform a Vulnerability Assessment. Assessments that are performed using internal company resources are useful for establishing baselines and to provide ongoing assessment. It is highly recommended that regularly scheduled vulnerability assessments are performed by an agnostic third party to independently verify internal results and confirm mitigation efforts.

For More Information on Reducing Your Risk

- Reference CIS Controls - Organization Section 7.1, control 3, Continuous Vulnerability Management.

PSA committee
CYBERSECURITY

Identify Appropriate System Topologies, Technologies & Policies to

Protect Your Systems, Network & Data

Network Requirements	Topology Considerations	Technology Considerations	Policy Considerations
Basic Risk	• CAT6 • WiFi/ BYOD • On Premise Firewall • UPS/ stateful shutdown	• Firewall • Guest Network • MFA • Patch Management • Backups • Bitlocker/ Defender	• Access Control • Acct. Management • Awareness/ Training • System Maintenance • Physical Security
Medium Risk	• Segmentation • VLAN (Azure/ AWS/ Google) • DNS	• VPN • MFA • MAC Filtering • MDM • Password Manager • Blacklist • Encryption Strength • Vulnerability scanning • Application scanning	• Audit & Accountability • Configuration Baseline • Identification/ Authentication • Personnel Security Controls • Media Protection • Acceptable Use • Password Construction & Rotation
High Risk	• **Audit/ As-Builts** • **IPv6** • **Domain Blocking (.ru)** • **SOC/ Monitoring** • **DDOS mitigation**	• **PKI/ Smart Cards** • **Data Loss Prevention** • **Application signing** • **Whitelist** • **Intrusion Detection/ Prevention** • **SIEM** • **Endpoint Detection & Response** • **Privileged Access Management**	• **Incident Response** • **Contingency Planning** • **Risk Assessment** • **System Assessment** • **System Comm Protections** • **System Privacy** • **Data Classification** • **Disaster Recovery Plan**

PSA committee
CYBERSECURITY

Develop a **Comprehensive Incident Response Plan to Carry Out in the Event of Cyber Attack**

An incident response plan provides a means to identify, eliminate and recover from cybersecurity events. Following the plan, a group can quickly respond to a security event.

A sound incident response plan requires a team that will carry it out. This team is usually called the Computer Security Incident Response Team (CSIRT). The CSIRT is a group that collect, analyze and act upon information associated with an event. The CSIRT is also responsible for communicating with other organizational stakeholders and external parties.

Having an incident response plan (IRP) helps an organization prepare for an reduce the impact of security incidents. They can also have positive effects on an organization such as: data protection, reinforcement of reputation and reduces potential costs.

According to a 2019 study by IBM, the average cost of a breach is **$3.86 million** and take an average of **280 days to identify and contain.**

The SANS Institute's Incident Handlers Handbook defines six steps that should be taken by the CSIRT to effectively handle security incidents. A good IRP addresses each of these steps.

Preparation

This step includes defining and/ or reviewing the security plan that is the basis of the IRP. A risk assessment should be performed and security issues prioritized against the most important assets.

Questions that need to be answered include:

- How does the organization define a security incident?
- What key stakeholders are needed to respond to a security incident?
- Should the IRP include the entire organization, a business unit, or a department?

The scope of the plan will dictate who should be involved.

The members of the CSIRT as well as key stakeholders that will be involved with the IRP should be identified and trained. The stakeholders may include legal, public relations, human resources, physical security team, vendors, key business partners and senior management. The roles of each stakeholder also should be defined.

A communication plan should be created and document the roles, responsibilities and processes that will be used as part of the IRP.

Within the preparation phase, the developed plan should be something that will be used. The applicability of the plan can be explored with the stakeholders to see if needed scenarios are included in the plan.

Identification

The team should be able to effectively detect or identify events within the environment that are outside normal operation.

When a potential incident is discovered, the appropriate stakeholders should be notified. The IRP should include a communication plan and escalation matrix. Who should be told what and when is important to the overall management of an event.

The incident should be analyzed. The analysis should address the "who, what, where, why and how" to provide additional information in addressing the root cause and later steps within the IRP.

Where possible, "playbooks" should be created to follow during an event. Playbooks could be developed to address malware, denial of service, unauthorized access, etc. Playbooks would include how an incident is detected, what stakeholders would be involved, standard response tasks, and when the incident could be resolved.

Containment

The immediate goal after discovering the incident should be to contain it and prevent additional damage.

This could include steps such as isolating the affected network or servers and applying fixes and/ or patches.

Eradication

The CSIRT should identify the root cause of the event, remove the threat and work to prevent similar attacks in the future.

Recovery

In the recovery phase, the team will bring affected systems back into production while monitoring to prevent another incident from occurring. The recovery point and testing processes as well as monitoring the systems will all be important steps.

Lessons Learned/ Post-Incident Handling

In the final phase, the event should be reviewed and documentation of the full scope of the event, how it was contained and eradicated, steps that were effective, and what could be improved in the future so that the group can improve their response.

Incident Response Plan Examples

It may be useful to be able to reference an actual IRP when working to develop one for an organization. Some examples or sections may not be applicable in all cases but can be used as a start.

- TechTarget: https://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/SearchDisasterRecovery_Incident_Response_Plan_Template.doc
- Thycotic: https://thycotic.com/solutions/free-it-tools/free-privileged-account-incident-response-policy-template/ (requires registration)
- Sysnet: https://sysnetgs.com/security-incident-response-plan-template/ (requires registration)
- California Government Department of Technology: https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc
- Carnegie Mellon University: https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf
- Tulane University: https://ts.tulane.edu/computer-incident-response-plan
- Wright State University: https://www.wright.edu/information-technology/policies/incident-response-plan

References

- Incident Response Plan 101: How to Build One, Templates and Examples: https://www.exabeam.com/incident-response/incident-response-plan/
- SANS Incident Handler's Handbook: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- Cost of a Data Breach Study | IBM: https://www.ibm.com/security/data-breach
- 10 Steps to Develop an Incident Response Plan You'll ACTUALLY Use: https://engineering.salesforce.com/10-steps-to-develop-an-incident-response-plan-youll-actually-use-6cc49d9bf94c