An American “Whole Of Nation” approach to combating cybercrimes committed against government agencies, business organizations, the infrastructure, and utility companies.

Created by

Thomas Bronack, CBCP
bronackt@gmail.com
(917) 673-6992

Table of Contents

Table of Figures

Cybercrime costs must be addressed and reduced!

The global cost of cybercrimes currently requires 9.047% of the Global GDP to address and increasing every year (i.e. **$9.5 trillion** / **$105 trillion** x 100 = 9.047%). That represents $9.5 trillion spent on cybercrime defenses and responses.

Our dependency on the use of technology has resulted in an increased exposure to loss of IT services, with an impact that would cause the world economy to collapse. Nation States and experienced hackers are attacking governments, businesses, infrastructure, and utilities on an hourly and daily basis, while organizations implement defenses in months and quarters (through Patches and New Releases). This defense is a reactive approach to problem mitigation and a losing approach. We need to do better, but how?

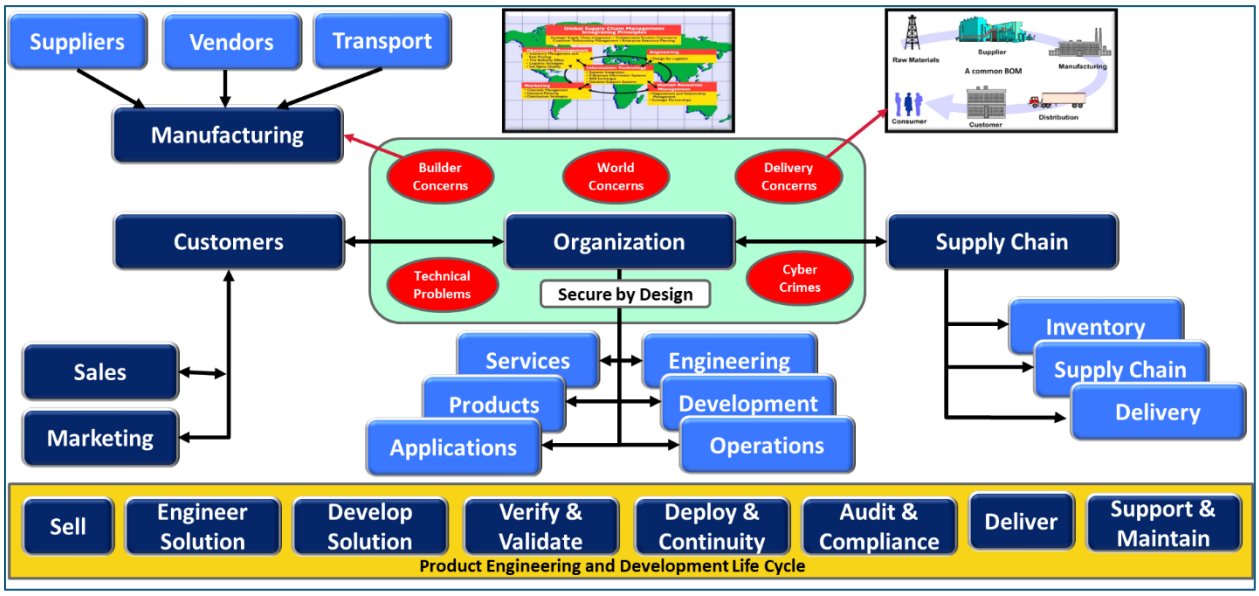


Figure 1: Protecting organizations, in a tumultuous world, is more difficult than ever!

Today organizations are conducting business on a global level and facing new challenges optimizing and defending their operations against technical problems and cybercrimes. The problem has risen to a level where a National and Global approach to defense must be adopted. In response the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (**CISA**) has developed an approach to protecting organizations through their “**Secure by Design**” pledge. This is a voluntary pledge focused on enterprise software products and services, including on-premises software, cloud services, and software as a service (SaaS). Physical products such as IoT devices and consumer products are not scoped in the pledge, though companies who wish to demonstrate progress in those areas are welcome to do so, but the FDA has already developed requirements governing medical device manufacturing and use. Also **DICOM** (for diagnostic information) and **IHE** for Integrating Healthcare Enterprises have been introduced to assist medical institutions deploy IT resources.

This article addresses the problems faced by organizations and provides an approach to implement a workflow that safeguards their organization and provides a vulnerability-free production environment.

Types of treats and sub-categories

Threats are separated into Groups, with categories and sub-categories as shown in the below illustration, which are:

- **Group 1** – Problems (Hardware, Software, and Procedures)
- **Group 2** – Solutions (Safeguards, Detections, and Responses)
- **Group 3** – Evidence (Project Plans, Artefacts, Transcripts, etc.)

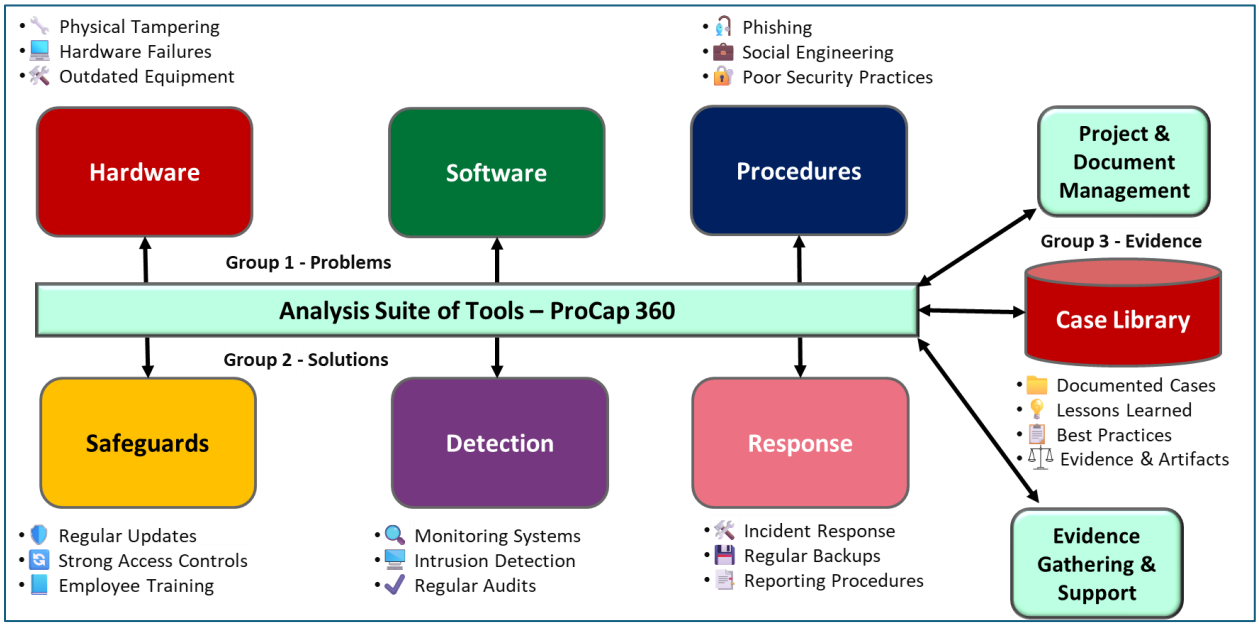


Figure 2: Threat Types and their sub-categories.

Following this methodology will allow you to proactively recognize cyber-attacks, technical problems, and outdated procedures. Safeguards can be created to detect flaws in workflow, products, services, and applications and responses can be taken to mitigate/mediate issues when they are discovered (Alarm, Problem Ticket, Alert, Actions taken and problem tracking until solved, then stored in problem library for future reference). This process eliminates potential errors prior to their introduction to the production environment.

A global approach to controlling cybercrimes.

A global approach to fighting cybercrimes has been in place for years, yet the nation-state and individual hackers are still ahead of the game. We must adjust our direction and put more effort into combating cybercrimes now more than ever. World tensions, physical access to critical materials and assets are in jeopardy and impacting business supply chains. Cybercrime is now a tool of destruction, like a bomb

would be. Luckily, new directions, laws, and policies have been introduced to assist government, businesses, infrastructure, and utilities fight against the cybercrime and technical threats we are facing.

A “Whole of World” approach is depicted in this illustration.

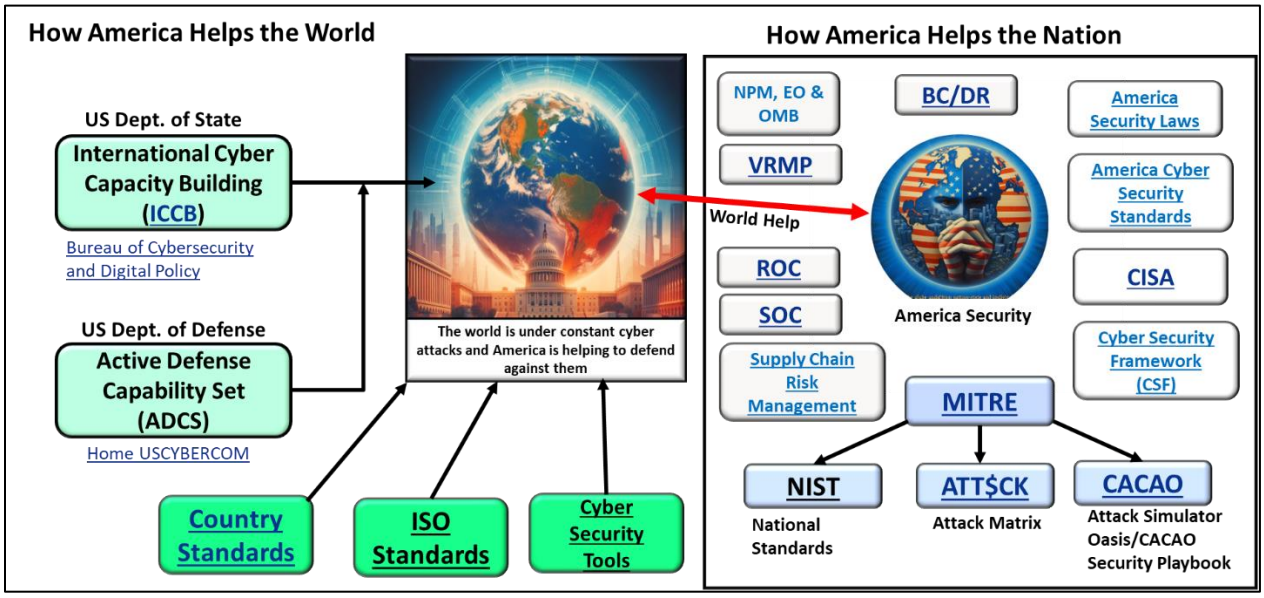


Figure 3: How America is assisting the World and itself in the fight against cybercrime

The new American approach to protecting against cybercrimes and technology threats includes the CISA (the Cybersecurity and Infrastructure Security Agency) announcement of a “Secure by Design” approach to developing new applications, Executive Order 14028 and Office of Management and Budget (OMB) memorandums require that a Software Bill of Materials (SBOM) is required to assist in ensuring only vulnerability-free applications are accepted in Information Technology (IT) production environments. Even the SEC has created a new rule (2023-139) that requires the Board of Directors inform them of any material breach related to cybercrime or technical problem that may impact shareholders and investors.

America has been assisting countries like Albania and Cost Rica for years through the Department of Defense and State Department to protect against cyber-attacks that threaten their societies. We are now addressing our own problem in a more diligent manner through the introduction of new policies, presidential memorandums, executive orders, direction statements, with stiff penalties and fines if not adhered to. These topics will be explored in more detail within this document, with links provided to access even more detailed information for those wanting to learn even more about a topic.

American companies are forming teams to address their vulnerability to cybercrimes and technical threats, with plans to assign individuals to newly created positions that define, create, and maintain a Vulnerability Risk Management Policy (**VRMP**) and Resilience Operation Center (**ROC**) responsible for being a single force within a company dedicated to vulnerability management and compliance.

Defending against cybercrimes and technical problems is everybody’s concern.

Cybercrime is expensive and harmful to governments, businesses, and the infrastructure. As world turmoil increases, it is even more important to safeguard your organization against cyber-attacks that could interfere with the continuity of your services and products.

How do we cope with the ever-rising costs of cybercrime on world economics and interruptions to the continuity of government, business, utilities, and the infrastructure. How can we better control the supply chain when malware, world tensions, and natural disasters are causing interrupts?

In 2024, cybercrime is predicted to cost the world a staggering **$9.5 trillion USD**[1]. The global GDP for 2024 is projected to be approximately **$105 trillion USD**[1]. Do you realize that 9.047% of Global GDP is spent combating cybercrimes and their impact (i.e., **$9.5 trillion** / **$105 trillion** x 100 = 9.047%).

Figure 4: Management is committing to proactively fighting cybercrime!

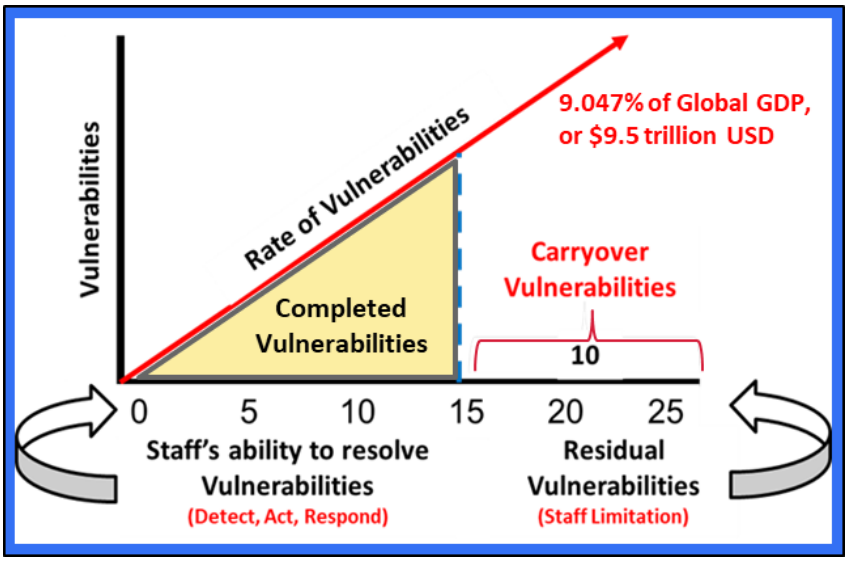


Figure 5: The Costs and Time Spent reacting to Vulnerabilities is costing 10.24% of Global GDP.

It is time we take action to curtail hackers and reclaim the funds currently spent on battling these disruptions, so that we can put those funds into more productive services.

Companies, Governmental Agencies, Utilities, and Infrastructure firms are spending time and energy responding to vulnerabilities that are injecting cybersecurity incidents and disrupting the supply chain, resulting in personnel burnout, high turnover, increased costs, and reputational damage to the organization, and increased threats to the public.

Types of Malwares.

Cybercrimes cause viruses and other types of malicious operations, commonly referred to as Malware. The most common types of **malwares** that you might encounter are shown below. Let us explore the most common types of malwares.

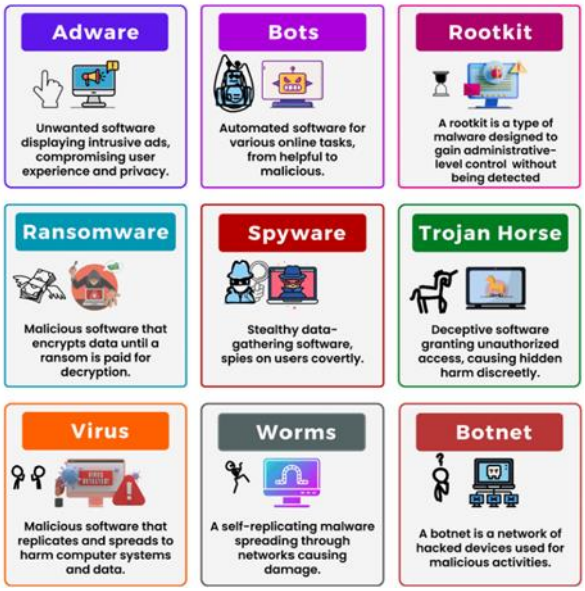


Figure 6: Types of Malware explained

1. **Ransomware**: This type of malware encrypts a victim’s data and demands a ransom payment to unlock it. For example, the city of Baltimore was hit by the **RobbinHood** ransomware, which disrupted city activities and cost millions of dollars.
2. **Fileless Malware**: Unlike traditional malware, fileless malware does not install anything initially. Instead, it modifies legitimate operating system files (such as PowerShell or WMI) to execute its malicious code. An example is the **Astaroth** campaign, which used legitimate Windows tools to steal credentials.
3. **Spyware**: Spyware collects user activity data without their knowledge. It can capture sensitive information like passwords and payment details. An example is the **DarkHotel** spyware.
4. **Adware**: Adware displays unwanted advertisements to users. One well-known example is the **Fireball** adware.
5. **Trojans**: Trojans disguise themselves as desirable code but perform malicious actions. The **Emotet** Trojan is a notable example.
6. **Worms**: Worms spread through networks by replicating themselves. The infamous **Stuxnet** worm targeted industrial control systems.
7. **Rootkits**: Rootkits give hackers remote control over a victim’s device **Zacinlo** is an example of a rootkit.
8. **Keyloggers**: Keyloggers monitor users’ keystrokes, capturing sensitive information **Olympic Vision** is a known keylogger.
9. **Bots/Botnets**: Bots launch large-scale attacks. The **Echobot** botnet is an example.
10. **Mobile Malware**: This infects mobile devices **Triada** is a notable mobile malware.
11. **Wiper Malware**: Wiper malware erases user data beyond recovery **WhisperGate** is an example.

Remember to stay vigilant and protect your devices against these threats!

Endpoint protection via EDR

Network endpoints allow staff, clients, vendors, and others to access your services via the internet. Violations to endpoint can result in cybercrimes and technology threats. Protections must be

implemented in your network design to protect sensitive data from unauthorized intruders. A four-step approach his recommended and presented within this document, which is:

1. **Discovery and Analysis** – Inventory and protection requirements for Automated Detection and Response.
2. **Selection and Planning** – Tools, Procedures, and Evaluations to optimize performance.
3. **Deployment and Configuration** – Staged Deployment and Roll-Back, Education, Configuration Optimization.
4. **Monitoring and Maintenance** – SIEM and Vulnerability Monitoring, Automated Patching, and Continuous Threat Exploitation Management.

Figure 7: Hackers are targeting American Infrastructure

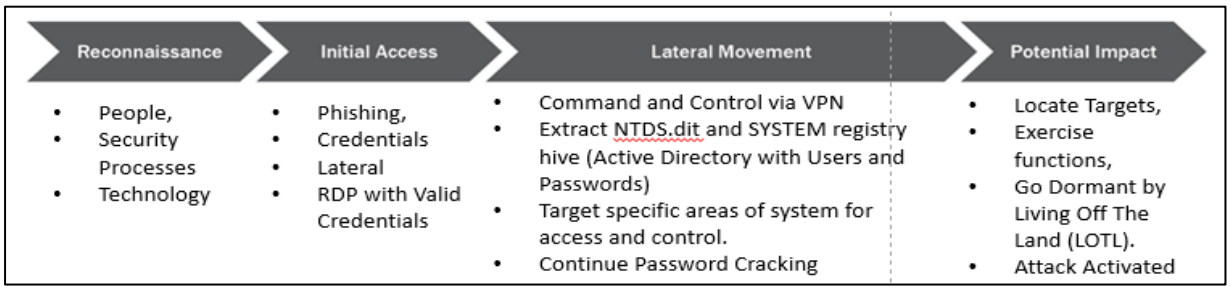


Figure 8: Process of Hacking with Live-Off-The-Land exploitation.

End-Point Security is Complex and Complicated, but Essential.

Performing endpoint protection includes the following steps.

1. **Know your Network** (Inventory and CMDB)
2. **Identify your Endpoints**.
3. **Protect Against** Cyber-crimes and Technical Problems.
4. **Implement best products** suited to organization and staff, including deployment and rollback.
5. **Implement anti-virus, malware, and vulnerability** products through best intrusion protections.
6. **Identify Spyware**, viruses, and malware.
7. **Scan to locate vulnerabilities in devices and programs** and provide application blocking.
8. **Develop policies** and audit schedules.
9. **Implement automated** patching and problem mitigation products.
10. **Implement Continuous** Threat Exploitation Management (CTEM) product.
11. **Create monitoring** and reporting dashboard.
12. **Provide extensive Awareness and Training** programs with career pathing.

Disaster Recovery for Medical Organizations and Hospitals

During emergencies, our medical services (hospitals, Emergency Medical Technicians, pharmaceuticals, etc.) will be essential to supporting lifesaving services for the public, therefore disaster recovery planning is crucial for healthcare organizations to ensure continuity of operations during and after emergencies. Let us explore key considerations and guidelines for creating an effective disaster recovery plan in the healthcare sector:

1. **Types of Disasters:**
    - Healthcare organizations should consider types of disasters that could impact their operations. These may include:
        - **Earthquakes:** Can cause care-related emergencies, equipment failures, power outages, and communication interruptions.
        - **Hurricanes:** Like earthquakes, hurricanes can disrupt operations, damage facilities, and lead to power loss.
        - **Severe Weather:** Extended severe weather conditions may affect transportation and lead to healthcare emergencies.
        - **Fires:** Both natural and human-caused fires can significantly impact operations.
        - **Disease Epidemics:** Outbreaks like the Ebola Virus Disease (EVD) can strain healthcare systems.
2. **Advance Planning:**
    - Develop a comprehensive disaster management plan that covers all aspects of healthcare operations.
    - Consider mission-critical applications and data, data backup plans, and HIPAA compliance.
    - Create a Business Continuity Plan (BCP) that outlines risk assessment, analysis of needs, and contingency planning.
3. **Disaster Recovery Plan Components:**
    - **Data Backup Plan:** Regularly back up critical data to ensure its availability during and after disasters.
    - **Emergency Mode Operations Plan:** Define procedures for operating in emergency mode, including access to essential resources.
    - **Education and Training:** Train staff in disaster preparedness, response, and recovery.
    - **Communication Plan:** Establish communication channels for internal and external stakeholders.
    - **Release of Information:** Determine how to manage patient information during emergencies.
    - **Staffing and Continuity of Care:** Locate, communicate with, and manage staff during disasters.
    - **Patient Advocacy:** Assist patients in recovering their health information.
    - **Practicing and Drills:** Conduct tabletop exercises and drills to evaluate the disaster plan.
4. **Recovery Planning:**
    - Recovery plans should be developed before a disaster and implemented during the response phase.
    - They support healthcare facilities in returning to normal operations or establishing a new normal state.
    - Consider financial viability and continued care for the community.

Remember that disaster recovery planning is not only essential for compliance but also critical for ensuring patient safety and maintaining healthcare services during challenging times.

Medical Building Management Systems

1. **Medical Building Management Systems (BMS**
   Healthcare facilities are complex environments that require efficient management of various systems. BMS, also known as Building Automation Systems (BAS), play a crucial role in healthcare settings.
   - **Purpose of BMS in Healthcare:**
     - **Efficient Operations:** BMS helps manage critical building functions such as heating, ventilation, air conditioning (HVAC), lighting, and security. It ensures optimal performance, energy efficiency, and occupant comfort.
     - **Granularity:** Unlike older systems that controlled entire buildings or floors, modern BMS operates at a room-by-room level. This adaptability is essential for healthcare facilities with diverse needs and operating hours.
     - **Energy Savings:** BMS optimizes HVAC, lighting, and other systems, reducing energy consumption. It can also confirm if energy comes from renewable sources.
     - **Resilience:** BMS contributes to building resilience by identifying hidden issues, improving maintenance, and ensuring continuity during disasters.
   - **Key Considerations:**
     - **Adaptability:** BMS must accommodate changes in building use and operational needs.
     - **Data Collection:** Sensors provide valuable data for localized environmental services.
     - **Sustainability:** BMS supports environmental goals by optimizing energy usage and reducing waste.
2. **Protecting Buildings During a Disaster Event:**
   - While natural disasters are often unavoidable, initiative-taking measures can mitigate damage and protect occupants:
     - **Flood Protection:**
       - Install flood barriers, such as sandbags or cofferdams, to prevent water infiltration.
       - Elevate critical equipment and utilities above potential flood levels.
     - **Wind and Storm Protection:**
       - Reinforce building frameworks to withstand intense winds (e.g., using heavy structural steel components).
       - Cover windows with wood or hurricane shutters to prevent damage.
     - **Fire Safety:**
       - Implement fire-resistant materials and fireproofing measures.
       - Regularly inspect and maintain fire suppression systems.
     - **Security Systems:**
       - Integrate security systems with backup generators to ensure continuous monitoring during power outages.
     - **Disaster Recovery Plans:**
       - Develop comprehensive disaster recovery plans that address evacuation, communication, and resource allocation.
       - Train staff in emergency procedures and conduct regular drills.

- **Resilient Construction:**
  - Construct hazard-resilient buildings capable of remaining functional during and after disasters.

Remember that an integrated approach, combining technology, planning, and resilient construction, is essential for safeguarding healthcare facilities and their occupants during disaster events.

New Laws and Legislation:

Nation-State and individual hackers are pursuing their trade on an hour-to-hour and daily basis, while application development and maintenance is pursued on a monthly or quarterly basis, which allows hackers to research posted vulnerabilities and take advantage of them before companies can mitigate vulnerabilities through patches or new releases. We must improve response times through **automation and artificial intelligence**.

Another critical aspect of fighting cybersecurity is a coordinated effort on the part of government, business, utility, and infrastructure companies. We must combine our efforts into a cohesive approach that will best defeat hackers and stop wasting funds on redundant or competitive tasks. We must also provide physical security to control access and prevent illegal intrusion determined to cause damage.

Recently a “**Whole-of-Nation**” approach to fighting cybersecurity has been announced as a National Policy Memorandum (**NPM-22**), while a new approach to developing applications and providing services was announced by CISA as a “**Secure by Design**” methodology to insure that security is built into applications, services, and consumer products.

Figure 9: Personnel are being trained to fight cybercrimes and technology threats!

The SEC New Rule and other laws introduced for greater protection against cybercrimes.

The Securities and Exchange Commission has recently mandated a new rule (**SEC New Rule 2023-139**) to protect shareholders and investors. This rule requires the Board of Directors to inform the SEC within five business days of any material breach that could impact the shareholder or investor financials and/or continuity of their company (with civil, criminal, and personal liability assigned as punishment for failure to obey this rule).

Executive Orders have been produced to mandate vulnerability-free applications in the production environment (**EO 14028**) and backed up by memorandums from the Office of Management and Budget (OMB **M-22-18** / **M-23-16**) that are designed to protect the software supply chain. Additionally, the Food and Drug Administration (FDA) has introduced new guidelines that require an SBOM for all medical devices to ensure that their origin is known, along with the manufacturer and component owner (**FDA SBOM Requirement Rule**). These new OMB memorandums also require the use of a Software Bill of Material (SBOM) to track the origin and component owners of software products

used to support applications in the cloud environment (i.e., Open-Source, Vendor, etc.,) as an aid to insure a vulnerability-free production site.

Secure by Design – Definition, description, and usage examples

Secure by Design, as proposed by the **Cybersecurity and Infrastructure Security Agency (CISA)**, refers to an approach where technology products are intentionally designed and built with security in mind from the outset. The goal is to create systems and devices that inherently protect against cyber threats, rather than trying to add security features as an afterthought.

Here are key principles of Secure by Design:

Risk Assessment: Before developing any technology product, a thorough risk assessment should be conducted. This involves identifying potential security risks, threat vectors, and vulnerabilities. By understanding these risks early in the design process, developers can make informed decisions to mitigate them. This could be the foundation for a Vulnerability Risk Management Policy based on Secure by Design.

Least Privilege: Systems should be designed with the principle of least privilege. This means that users, applications, and processes should only have the minimum necessary permissions to perform their tasks. Unnecessary privileges increase the attack surface and potential for exploitation.

Defense in Depth: Secure by Design emphasizes multiple layers of security controls. Instead of relying solely on a single security measure, a layered approach ensures that even if one layer fails, other layers can still provide protection. Examples include firewalls, intrusion detection systems, and encryption.

Default Secure Configurations: Devices and software should come with secure default configurations. Users should not need to disable security features or change settings to achieve a baseline level of security. Manufacturers and developers should set secure defaults to minimize the risk of misconfigurations.

Secure Communication: Communication channels between devices, networks, and services should be encrypted using strong cryptographic protocols. Secure communication prevents eavesdropping, data tampering, and unauthorized access.

Regular Updates and Patching: Secure by Design products should have mechanisms for regular updates and patches. This ensures that known vulnerabilities are addressed promptly. Automatic updates can help keep devices secure without relying on user actions.

Authentication and Authorization: Robust authentication mechanisms (such as multi-factor authentication) and proper authorization controls are essential. Only authorized users should have access to sensitive functions or data.

Privacy Considerations: Privacy should be part of the design process. Systems should minimize the collection and retention of personal data, and privacy-enhancing features should be incorporated.

Secure Boot and Firmware: Ensuring the integrity of boot processes and firmware is critical. Secure boot mechanisms prevent unauthorized code execution during system startup.

Threat Modeling: Developers should perform threat modeling exercises to identify potential threats and attack vectors specific to their product. This helps inform design decisions and security features.

Remember that **Secure by Design is an ongoing process**. As threats evolve, so should the security measures. By adopting this approach, organizations can create more resilient and trustworthy technology products.

Organizations are voluntarily taking the **CISA Secure by Design pledge** to publicly agree to adopt three principles:

- Take ownership of customer security outcomes,
- Embrace radical transparency and accountability, and
- Lead from the top by making secure technology a key priority for company leadership.

Examples of how Secure by Design can be used include:

Here are examples of **Secure by Design** practices that organizations and developers can adopt to enhance the security of their products and systems:

1. **Secure Defaults**: When designing software or hardware, set secure defaults for configurations. For instance:
    - **Network Devices**: Ship routers and switches with strong default passwords, disable unnecessary services, and enable security features like firewalls.
    - **Software Applications**: Ensure that default settings prioritize security (e.g., enabling HTTPS by default).
2. **Least Privilege**: Implement the principle of least privilege:
    - **User Accounts**: Limit user permissions to only what is necessary for their tasks.
    - **Application Permissions**: Apps should request only the minimum permissions required for their functionality.
3. **Authentication Mechanisms**:
    - **Multi-Factor Authentication (MFA)**: Encourage users to enable MFA to add an extra layer of security.
    - **Strong Password Policies**: Enforce password complexity rules.
4. **Secure Communication**:
    - **Transport Layer Security (TLS)**: Use TLS for encrypting data in transit (e.g., HTTPS for web traffic).
    - **Secure Protocols**: Avoid outdated or insecure protocols (e.g., SSL).
5. **Regular Updates and Patching**:
    - **Automatic Updates**: Enable automatic updates for software and firmware.
    - **Timely Patching**: Address known vulnerabilities promptly.
6. **Threat Modeling**:
    - **Identify Threats**: Conduct threat modeling exercises during the design phase.
    - **Mitigation Strategies**: Plan how to mitigate identified threats.
7. **Secure Boot and Firmware**:
    - **Secure Boot**: Ensure that only trusted firmware and software can run during system startup.
    - **Firmware Integrity Checks**: Regularly verify firmware integrity.
8. **Privacy Considerations**:
    - **Data Minimization**: Collect and retain only necessary user data.

- **Privacy-Enhancing Features**: Implement privacy features (e.g., anonymization, pseudonymization).

9. **Defense in Depth**:
   - **Layered Security**: Use multiple security layers (firewalls, intrusion detection systems, access controls).
   - **Redundancy**: Have backup systems in place. Use **air gap for vaulting** critical files to avoid ransomware infections of backup data. Use **immutable data** techniques.
10. **Security Testing**:
    - **Penetration Testing**: Regularly evaluate systems for vulnerabilities.
    - **Code Reviews**: Review code for security flaws.

Constantly review modern technologies and practices to update vulnerability management policy as modern technologies are enhanced and introduced.

How can a company implement Secure by Design?

An example of how a company can implement **Secure by Design** and the impact it has on the supply chain and clients.

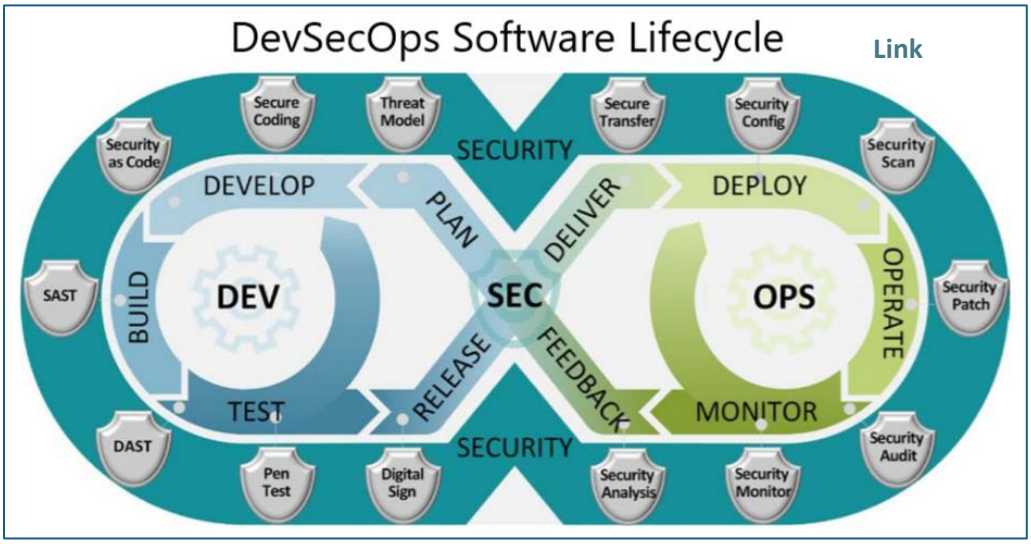
1. **Understanding Secure by Design**:
   - **Secure by Design** is an approach to software development that prioritizes security as a core business requirement rather than treating it as a mere technical feature or an afterthought.
   - In this approach, technology providers build security into the design process at every stage of a product’s development lifecycle. The goal is to identify and mitigate potential vulnerabilities before the product reaches the market.
   - 

Figure 10: Government suggest DevSecOps environment and phases.

   - The ultimate vision is to create a future where consumers can trust the safety and integrity of the technology, they use daily.
2. **Implementation Steps**:
   - **Executive Ownership**: Company leadership must take ownership of security. They should ensure that security is a fundamental consideration in product design, development, and deployment.

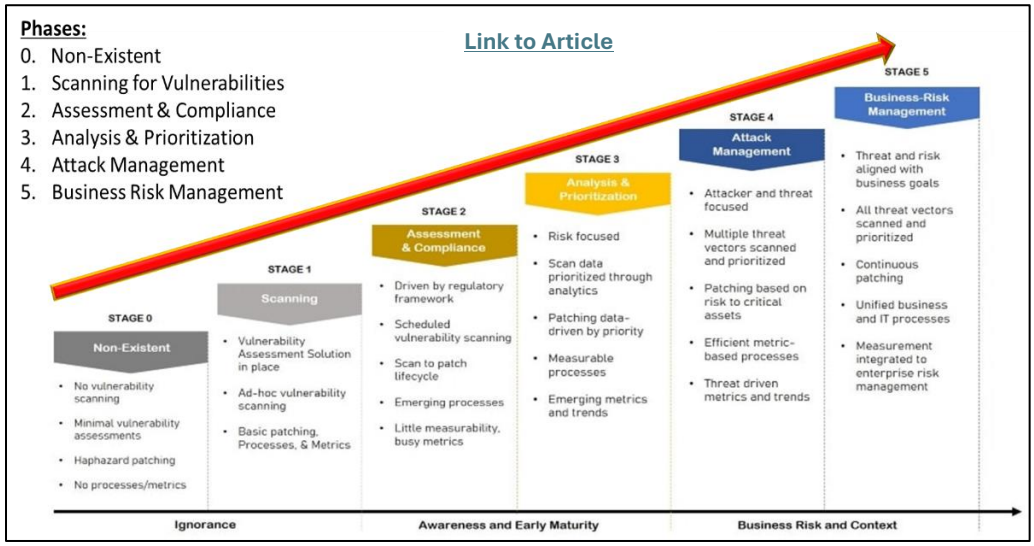
- **Secure Development Lifecycle (SDL)**: Implement an SDL that includes security assessments, threat modeling, secure coding practices, and regular security testing.
- **Vulnerability Management**: Continuously monitor and address vulnerabilities throughout the product lifecycle.
- 

Figure 11: Vulnerability Management Lifecycle phases and capabilities.

- **Secure Defaults**: Design products to be secure by default. This means they are resilient against common threats without requiring users to take additional steps.
- **Security Training**: Train developers and engineers on secure coding practices.
- **Third-Party Components**: Assess and secure third-party components used in the product.
- **Supply Chain Security**: Extend secure practices to suppliers and partners in the supply chain.

3. **Impact on Supply Chain and Clients**:
   - **Supply Chain**:
     - By adopting Secure by Design, companies reduce the risk of introducing vulnerable components into their supply chain.
     - Suppliers are expected to follow secure practices, leading to a more robust overall ecosystem.
     - Supply chain attacks become less effective because products are inherently secure.
   - **Clients**:
     - Clients benefit from products that are **secure-out-of-the-box**.
     - **Reduced reliance on post-purchase security measures** (e.g., patching, monitoring logs).
     - **Enhanced trust** in the safety and integrity of the technology they use.
     - Fewer exploitable flaws mean fewer cyberattacks and breaches affecting clients.

Secure by Design shifts responsibility from end users to technology manufacturers, creating a safer digital environment for everyone. Companies that embrace this approach strengthen their supply chain and build trust with clients.

SBOM creation and usage.

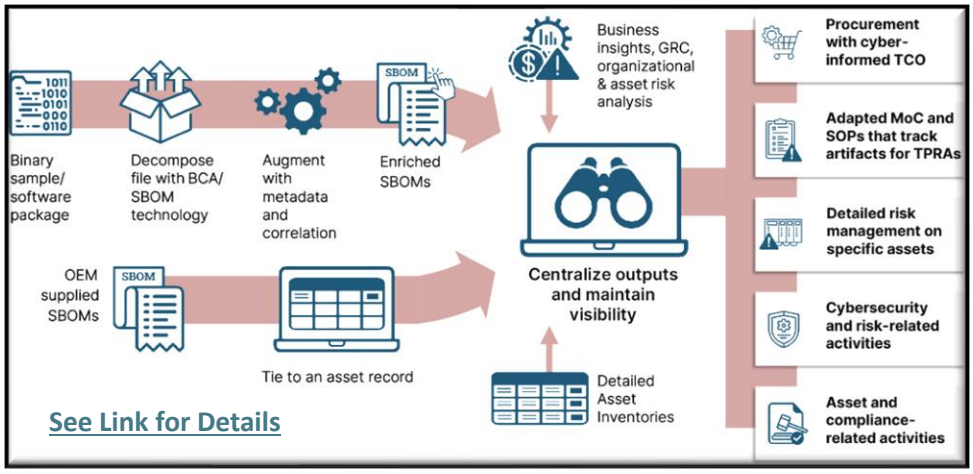


Figure 12: How a Software Bill of Material (SBOM) is created and used!

Software Bill of Materials – are lists of software components that are included in an application. Sometimes programs are embedded within other programs (like assemblies used to build cars) and these tiers may be multiple layers in depth. Each program will be checked to see if a vulnerability (CVE – Common Vulnerability Exploitation) is associated with the program / component. A Public Vulnerability Databases (National Vulnerability Database – NVD) is maintained by DHS, but there are other databases containing CVE’s and their explanation (i.e., Identifier, description, and mitigation as a patch or a new release), so it is important to know of **these databases** and include them in your vulnerability searches.

Using SBOMs to combat vulnerabilities has allowed the application test team to identify and mitigate program problems before they enter the production environment, thereby adhering to laws and improving the reliability of production operations. Combining vulnerability management with code testing programs (static, dynamic, interactive, and runtime) will further safeguard your organization.

Adding **immutable data technologies** and ensuring that an air gap is enforced between the data center and vaulted backup tapes is another means to protect your organization and will assist in recovering from a Ransomware attack. Producing periodic system snapshots will allow your organization to recover operations at the point where the snapshot was taken. If the snapshot is prior to the infection of a virus, it will support your recovery operation and eliminate the virus infection. You will have to perform a forward data recovery from the snapshot to the current system state before recovering operations can occur.

The requirements for Software Bill of Materials (SBOMs) have become increasingly important for both government and business organizations. Here are the key mandatory requirements and the reasons behind them:

What do SBOMs do

A Software Bill of Materials (SBOM) is a comprehensive list of all the software components, dependencies, and metadata associated with an application. It functions as an inventory of all the building blocks that make up a software product, allowing organizations to better understand, manage, and secure their applications.

SBOMs are crucial for ensuring software transparency, managing open-source software and third-party dependencies, and identifying and mitigating security vulnerabilities.

Federal regulations requiring SBOMs include the Executive Order on Improving the Nation’s Cybersecurity, which mandates federal agencies to collect software attestations and artifacts like SBOMs from government software vendors. This Executive Order directs the Department of Commerce, in coordination with the National Telecommunications and Information Administration (NTIA), to publish the minimum elements for an SBOM. Additionally, the Office of Management and Budget (OMB) has issued a memorandum stating that federal agencies may require SBOMs in solicitation requirements. The Senate’s draft of the fiscal 2023 National Defense Authorization Act also authorizes the Secretary of Defense to require SBOMs for all noncommercial software created for or acquired by the Department of Defense.

Those who must follow SBOM regulations include federal agencies and their contractors, as well as software suppliers that sell to U.S. federal government agencies. This requirement is aimed at enhancing the security of the software supply chain and ensuring compliance with secure development practices.

Other standards and guidelines that require SBOMs include the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA), which impose rules regarding the security of software components that collect and process data. However, PCI DSS explicitly uses the term SBOM and requires an inventory of software components, while HIPAA does not specifically mention SBOM but emphasizes the security of software components. The three most popular SBOM standards accepted by the U.S. government are CycloneDX, Software Identification (SWID) tag, and Software Package Data Exchange (SPDX). These standards provide a common format for describing the composition of software in a structured way that is consumable by other tools, such as vulnerability scanners.

In the United States, several regulations and directives mandate the use of Software Bill of Materials (SBOMs) for both business and government organizations:

1. **Executive Order 14028**: Issued in May 2021, this order directs the National Institute of Standards and Technology (NIST) to develop guidelines for creating and publishing SBOMs. It also establishes criteria for using SBOMs in federal procurement processes.
2. **Cybersecurity and Infrastructure Security Agency (CISA)**: CISA recommends using SBOMs as part of its guidelines for secure software development.
3. **National Defense Authorization Act (NDAA)**: The Senate’s draft of the fiscal 2023 NDAA authorizes the Secretary of Defense to require SBOMs for all noncommercial software created for or acquired by the Department of Defense.
4. The FDA is mandating that all medical devices running software must create and maintain a Software Bill of Materials (SBOM) and will start enforcing that rule on Oct. 1, 2023.

These regulations aim to enhance software security and transparency, helping organizations manage software supply chain risks more effectively.

Mandatory Requirements for SBOMs

1. **Data Fields**: SBOMs must include specific data fields such as component name, version, supplier, and dependency relationships. This ensures comprehensive visibility into the software components.
2. **Standardized Formats**: SBOMs must be in one of three standardized formats—SPDX, CycloneDX, or SWID tags. This standardization allows for machine readability and interoperability across different systems.
3. **Automation Support**: SBOMs should support automated generation and updating processes. This helps in maintaining up-to-date records with each new software version.
4. **Self-Attestation**: U.S. agencies require software producers to provide a self-attestation of the SBOM and documented processes to validate code integrity.

Reasons for Mandating SBOMs

1. **Enhanced Security**: SBOMs provide detailed visibility into the software supply chain, helping to identify and mitigate vulnerabilities. This is crucial for preventing supply chain attacks like those seen with SolarWinds and Kaseya.
2. **Transparency**: By listing all software components, SBOMs promote transparency, allowing organizations to understand what is in their software and how it might be affected by vulnerabilities.

Figure 13: SBOM fields

3. **Compliance**: Government mandates, such as the 2021 U.S. Executive Order to Improve the Nation’s Cybersecurity, require SBOMs to ensure that software used by federal agencies meets security standards.
4. **Risk Management**: SBOMs help organizations manage risks by providing a clear inventory of software components, making it easier to track and address potential security issues.

Secure by Design emphasizes the importance of integrating security measures throughout the software development lifecycle. When it comes to SBOMs (Software Bill of Materials), Secure by Design highlights several key points:

Key Points on SBOMs from Secure by Design

1. **Visibility and Transparency**: SBOMs provide a detailed inventory of all software components, which is crucial for identifying and managing vulnerabilities. This transparency helps in understanding the software’s composition and potential risks.
2. **Proactive Risk Management**: By maintaining an up-to-date SBOM, organizations can proactively manage risks associated with third-party components. This includes tracking known vulnerabilities and ensuring timely updates and patches.

3. **Compliance and Standards**: Secure by Design advocates for adherence to industry standards and regulatory requirements. SBOMs help organizations comply with these standards by providing a clear and auditable record of software components.
4. **Supply Chain Security**: SBOMs enhance supply chain security by allowing organizations to verify the integrity and origin of software components. This is essential for preventing supply chain attacks and ensuring the trustworthiness of software.
5. **Automation and Efficiency**: Secure by Design encourages the use of automated tools to generate and maintain SBOMs. Automation ensures that SBOMs are accurate, up-to-date, and can be easily integrated into existing security processes.

Why SBOMs are Mandated

- **Enhanced Security**: SBOMs help in identifying and mitigating vulnerabilities, reducing the risk of cyberattacks.
- **Transparency**: They promote transparency in the software supply chain, making it easier to understand and manage software components.
- **Compliance**: SBOMs help organizations meet regulatory requirements and industry standards.
- **Risk Management**: They provide a clear inventory of software components, aiding in effective risk management.

In summary, Secure by Design underscores the necessity of SBOMs for maintaining robust security practices, ensuring compliance, and managing risks effectively.

Endpoint Security is complicated, but critical to secure the organizations.

Network endpoints allow staff, clients, vendors, and others to access your services via the internet.
Violations to endpoint can result in cybercrimes and technology threats.
Protections must be implemented in your network design to protect sensitive data from unauthorized intruders.
A four-step approach his recommended and presented within this document, which is:

- **Discovery and Analysis** – Inventory and protection requirements for Automated Detection and Response.
- **Selection and Planning** – Tools, Procedures, and Evaluations to optimize performance.
- **Deployment and Configuration** – Staged Deployment and Roll-Back, Education, Configuration Optimization.
- **Monitoring and Maintenance** – SIEM and Vulnerability Monitoring, Automated Patching, and Continuous Threat Exploitation Management.

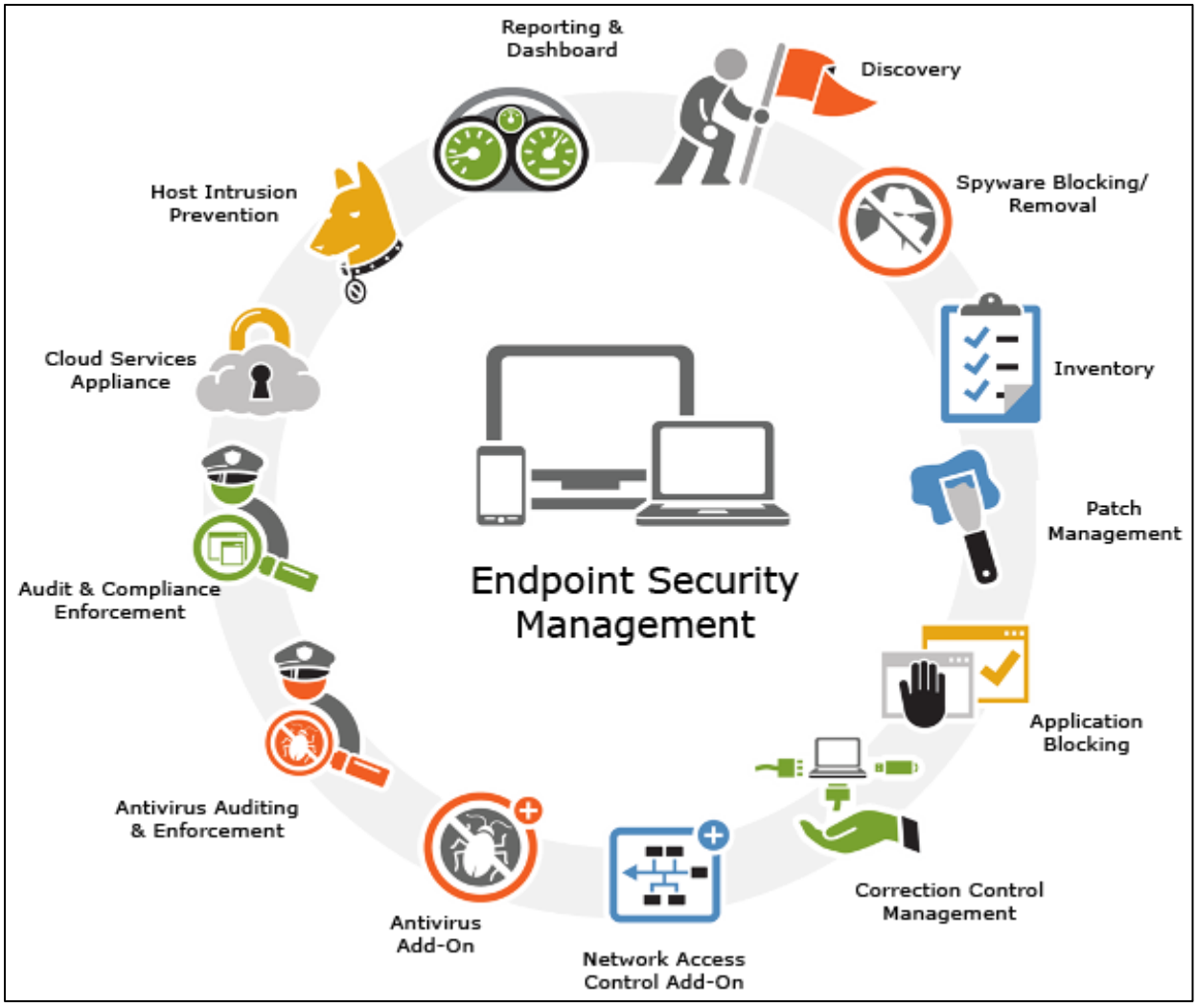


Figure 14: Endpoint protection is complicated, but essential.

The benefits received through endpoint security include:

1. **Know your Network** (Inventory and CMDB)
2. **Identify your Endpoints**.
3. **Protect Against** Cyber-crimes and Technical Problems.
4. **Implement best products** suited to organization and staff, including deployment and rollback.
5. **Implement anti-virus, malware, and vulnerability** products through best intrusion protections.
6. **Identify Spyware**, viruses, and malware.
7. **Scan to locate vulnerabilities in devices and programs** and provide application blocking.
8. **Develop policies** and audit schedules.
9. **Implement automated** patching and problem mitigation products.
10. **Implement Continuous** Threat Exploitation Management (CTEM) product.
11. **Create monitoring** and reporting dashboard.
12. **Provide extensive Awareness and Training** programs with career pathing.

Modern Technologies used to combat cybercrimes.

Innovative technologies have been introduced to help your organization produce a vulnerability-free environment and recover from encountered problems. These modern technologies are shown in the picture below.

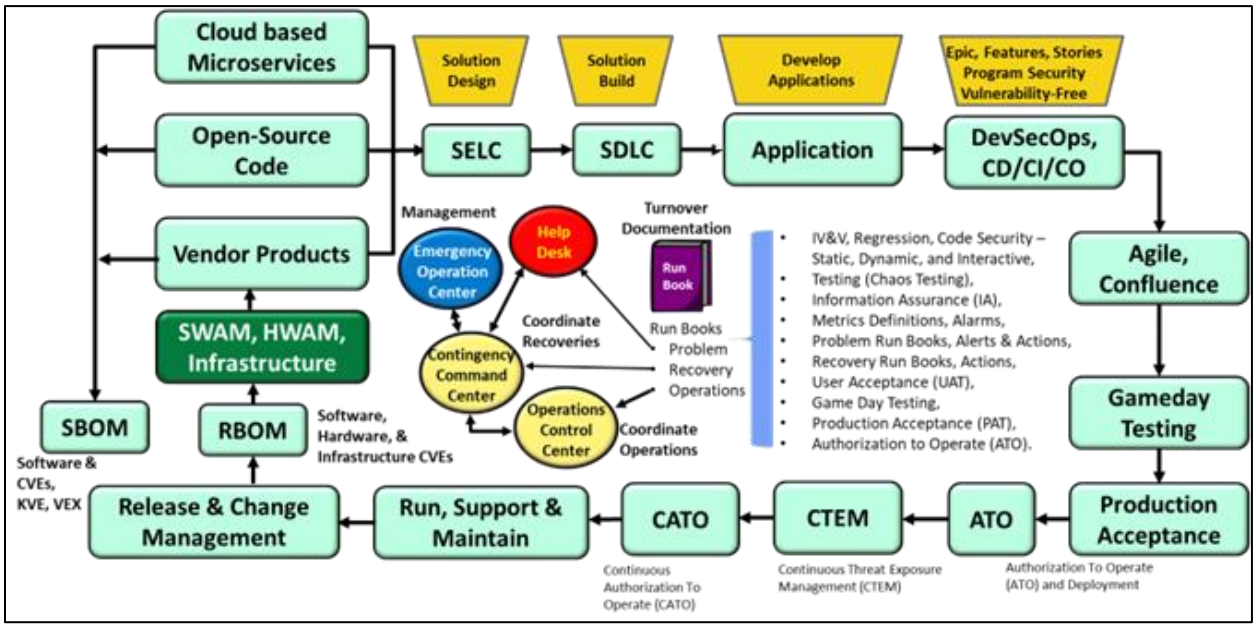


Figure 15: Producing vulnerability-free products and services through modern technologies!

The modern technologies include:

- **RBOM** – The Release Bill of Materials includes the software and infrastructure used by an application and will help the change management team judge the impact of a planned change. This is a proprietary product included in the **ProCap 360** product. It can be produced in a JSON format to support Infrastructure as Code (IAC) automation.
- **DevSecOps** – although not new DevSecOps includes code testing with vulnerability management to safeguard applications going through development or maintenance.
- **CTEM** – Continuous Threat Exposure Management *discovers, prioritizes, and validates potential risks and aligns remediation with business goals and compliance frameworks.* CTEM offers an initiative-taking and comprehensive approach to identify, prioritize, and mitigate risks while aligning remediation efforts with business objectives and compliance frameworks. By integrating tools such as penetration testing as a service (**PTaaS**), attack surface management (**ASM**), automated pen-testing, and **red-teaming**, CTEM ensures a proactive defense posture.
- **CATO**- Continuous Authorization to Operate can be achieved with approval by a third party to certify your ability to continuously provide vulnerability-free application through the development, maintenance, and production CTEM environments. The Risk Management Framework (**RMF**) establishes the continuous management of system cybersecurity risk and CATO is government’s method for validating that your organization is in continuous compliance and using best practices to protect the security of your operations.

- Using **Artificial Intelligence** to better locate potential virus attacks is helpful as well.

This **article** from SC Media will help to understand how to approach the mitigation of vulnerabilities within your organization.

Assigning problems to their component owner.

Another critical issue to be aware of is the need to identify every component owner (both internally and externally) so that problem reports can be responded to by the component owner. The sequence of events is:

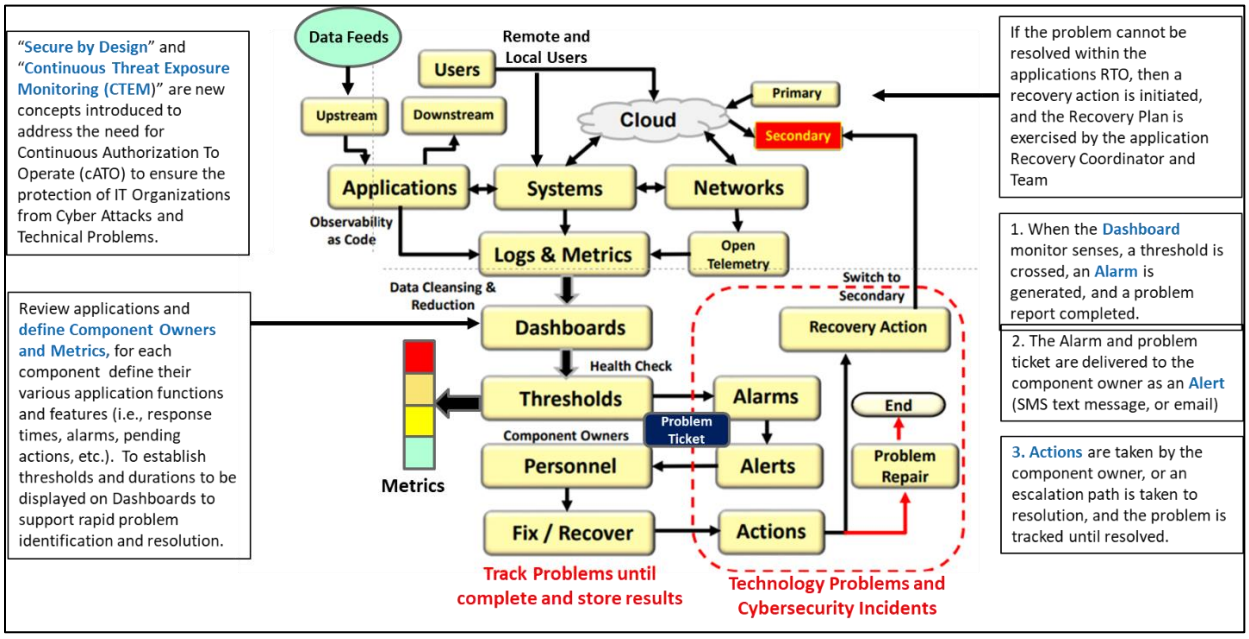


Figure 16: The Problem Management process and component owners!

- **Assign a metric** to a component and monitor activity against that component.
- **Establish Thresholds** and assign levels to the Threshold (Green, Yellow, Orange, Red) from good to bad.
- **Whenever a Threshold is crossed** for a predefined period, issue an alarm.
- **When the alarm is activated**, create a problem report and place the Alarm message into the body of the trouble ticket.
- **Route problem ticket to the component** owner as an alert.
- **The component owner takes actions** to mitigate the problem.
- **Escalations are performed to include experts in the mitigation process,** if necessary.
- **The problem ticket is tracked** from beginning to end by the problem management system.
- **A Problem Playbook** is followed to resolve the problem if one is available (**SOAR**), or Oasis’ Collaborative Automated Course of Operations (**CACAO**).
- **If the problem requires a recovery,** then a Recovery Runbook is followed and a system recovery is completed (Cold, Warm, or Hot Recovery).

- **The results of the problem are stored in the Problem Database** and can be accessed by personnel who want to review other problems of a similar nature for reference, or if a match is found, for mitigation.

What If the component owner is not known.

If you do not know who owns a component, then you will be at a loss when it comes to assigning a problem ticket and simple problems may linger for prolonged times. So it is important to know who owns a failing component. Internally, this problem can be resolved by assigning a component owner, but externally it may be extremely difficult to locate the owner of a component, especially when the component is embedded within an assembly of components to construct a program. For this reason, an SBOM is essential to locate components and define their owner. If your vulnerability search does not produce the owner of a component, then you may choose not to use that program.

How do you detect, rate, and mitigate vulnerabilities?

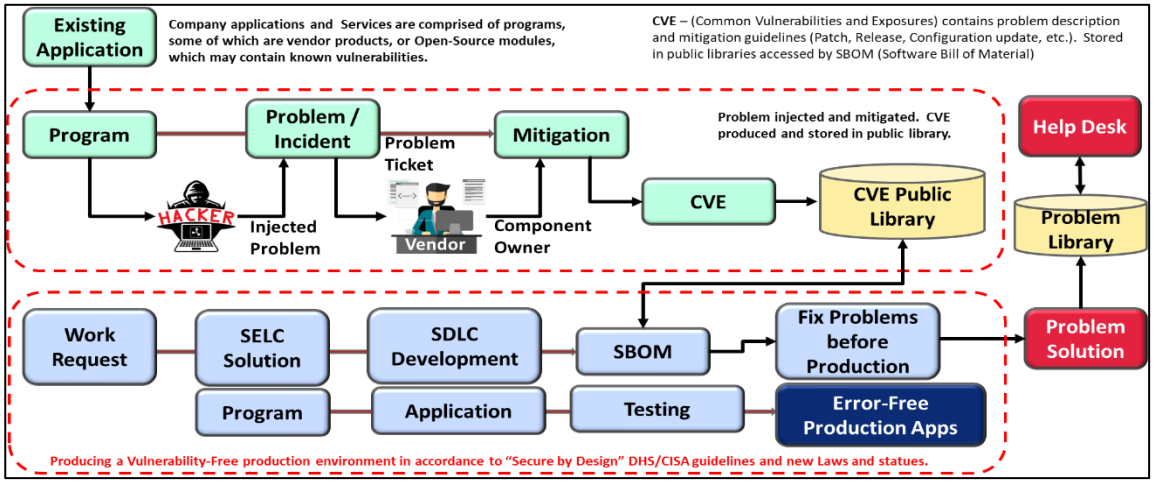


Figure 17: How vulnerabilities are researched and mitigated.

Whenever vulnerabilities are detected, they are analyzed and mitigated through a Root Cause Analysis (RCA) that provides a problem description, causes, and actions to be taken to resolve the problem or incident. These are named Common Vulnerability Enumerations (CVEs) and tracked from origination to resolution, then stored in a publicly addressable National Vulnerability Library. SBOMs examine the components contained within SaaS based and cloud applications to locate the programs composing cloud applications, vendor products, and services. The SBOM then examines the Public CVE Libraries to locate CVEs associated with the program so that technicians can repair any known vulnerabilities before production acceptance. This process will guarantee Vulnerability-Free production operations and adherence to new laws and regulations, along with reducing or eliminating cybercrime exposures.

When performing this process, an application security score may be determined, and thresholds used as gateways to govern the engineering, development, and maintenance process. The following display from ProCap 360 (an **Internet Infrastructure Services Corporation** product) will illustrate how you can define an applications security posture.

ProCap 360 displays Vulnerabilities and their Score.

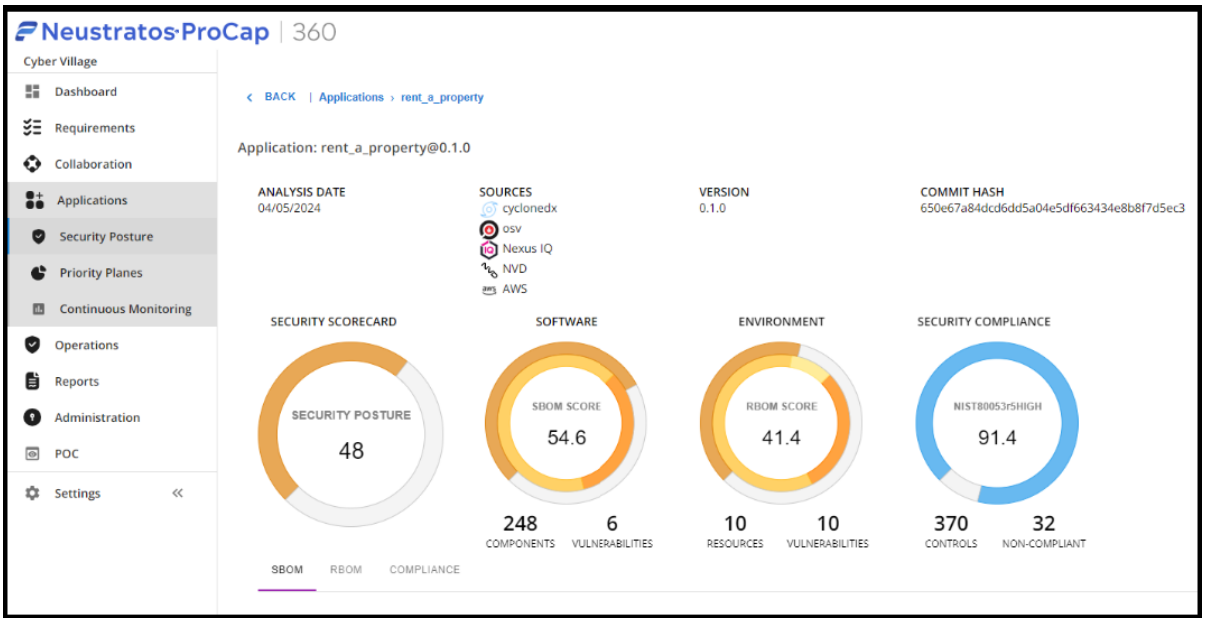


Figure 18: Acceptable vulnerability security scorecard for a Gateway to Production.

Vulnerability management tools like **ProCap 360** use SBOM components to calculate and communicate an application security score. In the example above, the Application Security Posture is forty-eight, the sum of SBOM Score and RBOM scores divided by two. The SBOM score is 54.6 across 248 components with six vulnerabilities. The environment score is 41.4, as shown by the RBOM Score, and the NIST800r5r5HIGH, which checks 370 controls and found 32 Non-Compliant. Applications can be examined in any environment (Development, Test, Production, etc.).

A drill-down screen provides programs that are included in the application. The application name is shown under the APP column. Its version is shown under the Version column, and the Last Analysis date is provided. The Sources column lists the public vulnerability databases that were searched to define this vulnerability. The are thirty-three components listed with their associated Vulnerabilities. Drill-down functions are provided to lookup the vulnerability, its identifier, description, and recommended mitigation.

Gates can be established to stop an application from leaving one development stage until it has achieved a specified Security Posture. Through this technique, you can control the development and maintenance of applications to adhere to vulnerability-free requirements.

The need to develop a Vulnerability Risk Management Policy:

With so many risks surrounding us, and a proliferation of tools, policies, and procedures that are used to combat technical problems and security incidents, it stands to reason that there is a need to develop a company-wide Vulnerability Risk Management Policy (VRMP) and to assign personnel to its development and maintenance going forward (Resilience Operations Center – ROC).

Conclusions based on present conditions.

This entire paper addressed the international and domestic cybersecurity problems faced by America and the world. It tried to make you aware of the tools and services available and the direction established to increasingly defend against harmful cybercrimes.

The conclusions arrived at within this paper.

1. Vulnerability Management must be considered and implemented.

   Vulnerability management is a process that organizations use to identify, analyze, and manage vulnerabilities within their operating environment. These vulnerabilities can exist in systems, platforms, infrastructure, or even people and processes.

   Examples of vulnerabilities include:

   - Insecure code,
   - Unpatched software,
   - Cloud misconfigurations,
   - Lack of encryption,
   - Default authentication,
   - Lack of security awareness and training, and
   - Improper internal controls.

2. Importance of Vulnerability Management:

   - Risk Management: Assessing the environment for technical and operational vulnerabilities helps organizations plan for and implement mitigating controls.
   - Comprehensive Understanding: Vulnerability management activities (such as discovering, categorizing, prioritizing, and analyzing vulnerabilities) provide insights into an organization’s risk profile.
   - Preventing Repeat Vulnerabilities: Effective vulnerability management prevents recurring vulnerabilities by addressing root causes.
   - Security and Compliance: It is a critical part of an organization’s overall security and compliance program.

3. Vulnerability Management Program:

   - A vulnerability management program is a structured approach adopted by companies to:
     - Identify, monitor, and remediate vulnerabilities.
     - Clearly define the process, structure, and scope of vulnerability management. Specify responsibilities and expectations for everyone within the organization.
   - A robust program helps organizations:
     - Prioritize vulnerabilities based on risk and exposure.
     - Prevent the introduction of known vulnerabilities.
     - Maintain compliance with security standards and regulations.

If you are interested in creating a vulnerability management policy for your organization, you can find customizable templates and examples online. Remember that having a well-defined Vulnerability Risk Management Policy is essential for effective vulnerability management!

Implementing a Vulnerability Management Policy

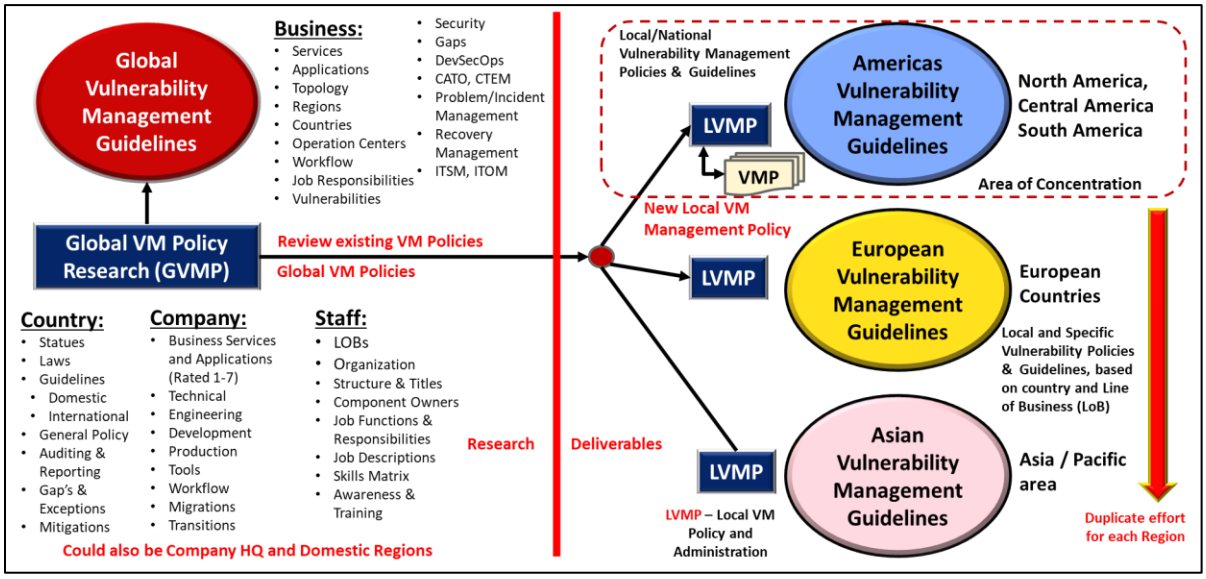


Figure 19: Implementing a Vulnerability Management Policy in organization.

A **Vulnerability Management Policy** outlines an organization’s approach to identifying, assessing, and mitigating vulnerabilities within its systems and processes. Here are the steps to create and maintain such a policy:

Define Scope and Objectives:

- Clearly state the purpose of the policy.
- Specify which assets (systems, applications, networks) fall under the policy’s scope.
- Set objectives, such as reducing risk exposure and maintaining compliance.

Risk Assessment:

- Regularly assess vulnerabilities using tools like vulnerability scanners and SBOMs.
- Prioritize vulnerabilities based on severity and potential impact.

Roles and Responsibilities:

- Define who is responsible for vulnerability management (e.g., IT teams, security personnel).
- Assign roles for vulnerability scanning, patching, and reporting.

Vulnerability Scanning and Assessment:

- Establish a schedule for regular vulnerability scans.
- Determine how often assessments occur (e.g., daily, weekly, monthly).

- Specify the tools or services used for scanning (i.e., ProCap 360).

Patch Management:

- Detail the process for applying security patches promptly (patch schedule).
- Address critical vulnerabilities first.
- Consider automated patch deployment.

Incident Response:

- Describe how to manage vulnerabilities that are actively exploited (**KVE** – Known Vulnerability Exploitation).
- Define steps for immediate remediation.

Reporting and Metrics:

- Specify reporting frequency (e.g., quarterly).
- Include metrics like vulnerability trends, time to patch, and risk reduction.

Review and Update:

- Regularly review the policy for relevance and effectiveness.
- Update it based on changes in technology, threats, or organizational structure.

Remember that a vulnerability management policy is dynamic—adapt it as needed to stay effective.

When considering a method for maintaining, updating, and training on Vulnerability Management, consider the development of a Resilience Operations Center (ROC) to coordinate all questions, responses, policies, documentation, awareness, and training related to Vulnerability Management as a sole source of knowledge to be provided to all personnel in the company upon demand. Should questions, or new conditions arise, then the ROC can research methods to mitigate and better control encountered or uncovered potential vulnerabilities.

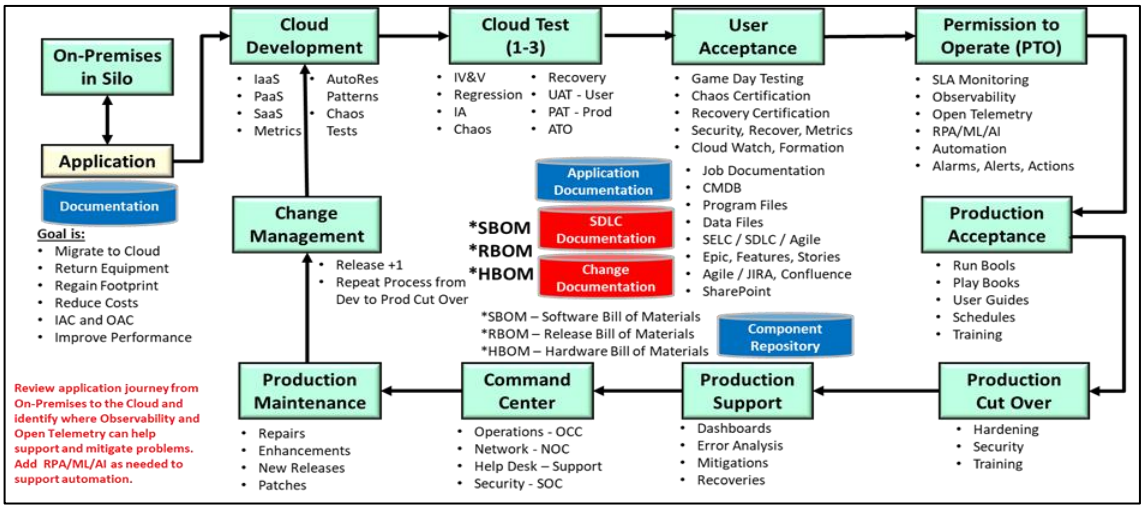


Figure 20: Process of Migrating Applications to the Cloud.

Performing an Audit and a Risk Assessment

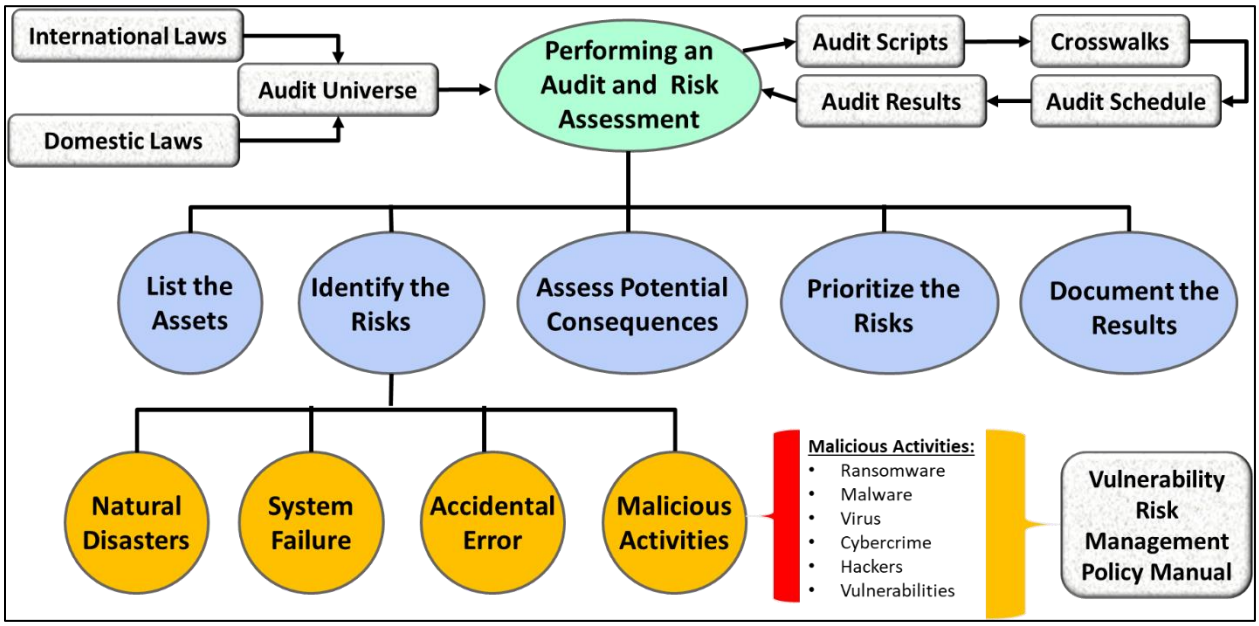


Figure 21: Performing an Audit and Risk Management Assessment

An **Audit** should include your exposure to international and domestic laws depending on the countries your organization conducts business in, while a **Risk Assessment** explore the occurrence of exposures that will require new controls to mitigate gaps and mediate exposures. The Vulnerability Risk Management Policy Manual contains the standards and procedures used to conduct everyday functions in adherence to Risk, Security, Engineering, Development, Operations, and Maintenance guidelines.

The **Vulnerability Risk Management Policy Manual (VRMP)**will be the repository of all actions performed in designing, engineering, building, developing, testing, accepting, deploying, and operating products, services, and applications used by or created by an organization.

Awareness and Training to management and staff is based on the VRMP and will be used to provide every level of staff with an awareness of vulnerability management and the actions needed to identify, report, respond to, and mitigate encountered cybercrimes and technology problems. Through these interactions an entire organization can build a resilient enterprise and take an initiative-taking approach to addressing the protections needed to maintain service continuity.

Securing Application Development, program code, and vulnerabilities

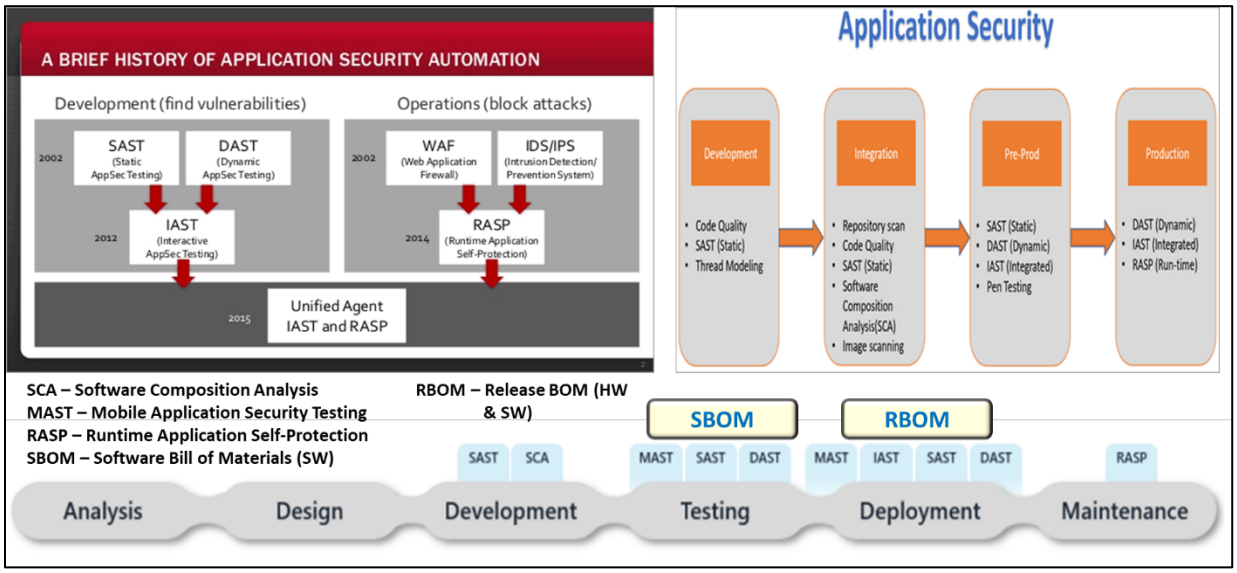


Figure 22: Securing application code and vulnerabilities to achieve DevSecOps.

Including Software code diagnostic tools for Static, Dynamic, Interactive, and Runtimes code testing will uncover weaknesses in code being developed or deployed. Using SBOM and RBOM technologies will uncover vulnerabilities in software programs and the infrastructure. Combining the two technologies will result in fewer software related problems and fewer costs related to staff toil and reputational damage due to encountered cybercrimes.

What new developments can we expect?

CISA’s ‘**Vulnrichment**’ program will focus on adding metadata to CVEs, including Common Platform Enumeration (CPE) numbers, Common Vulnerability Scoring System (CVSS) scores, Common Weakness Enumeration (CWE) nametags, and Known Exploited Vulnerabilities (KEV) entries (announced 5-8-2024).

With all the modern technologies and the change in direction for attacking cybercrimes, it is essential that an organization develop a **Vulnerability Risk Management Policy (VRMP)** to guide all levels of staff in the coordinated effort to eliminate vulnerabilities, wherever they may originate. A companion to the VRMP is a **Resilience Operations Center (ROC)** that would be responsible for addressing any concerns related to vulnerability management, maintaining the VRMP, and providing Awareness and Training classes to the staff.

The Resilience Operations Center (ROC)

The ROC is an extension of the military IROC or existing Global Security Operations Centers (GSOC) or other Operations centers that focus on vulnerability. The ROC will communicate with all areas within the organization and coordinate resilience operations. Any questions will be directed to the ROC staff, so a common database of resilience questions and responses can be maintained (FAQ – Frequently Asked

Questions), as well as the policies and guidelines developed by the organization to provide a vulnerability-free environment that better protects the organization against cybercrimes, viruses, and malware, resulting in a happier staff, less turnover, and a more informed and educated staff.

It is highly recommended that your organization review the topics covered in this paper and adopt those practices best suited to your needs.

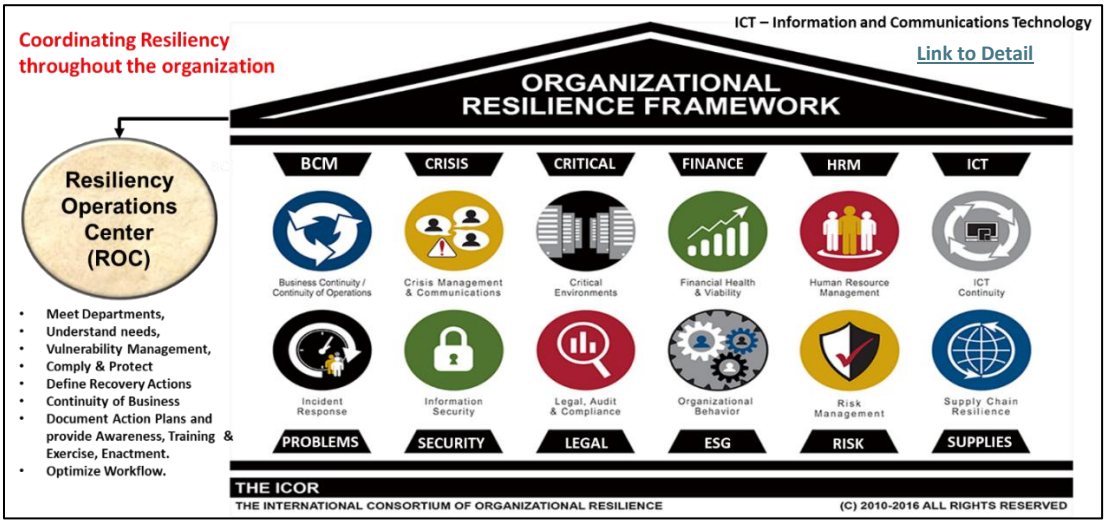


Figure 23: Coordinating vulnerability management within an organization.

Results received through “Secure by Design.”

After spending many months performing research, defining your requirements for a safeguarded and compliant environment that protects against cyber attacks and technical problems in a near real-time manner, formulating teams, and designing, developing, testing, deploying, supporting, and maintaining your ideal production environment, your organization will be best prepared to protect the continuation of you business and supplying of services to your customers.

The final goals will be to protect American government operations and facilities, businesses, utilities, and the infrastructure against technical problems and cyber threats.

Figure 24: Protecting America against technical problems and cyber threats.

Benefits from following the directions described in this document.

A reduction in costs and an improvement in efficiency and adherence to current laws and regulations can be achieve through the implementation of the following:

1. **Reduced costs and improved ability to protect against cybercrimes and technical problems.**
    - **a.** Reduced costs through automated identification and classification o vulnerabilities, prior to their entering the production environment (both for development and maintenance cycles) – thereby adhering to multiple laws and regulations with SBOM and RBOM technologies.
    - **b.** Improved staff efficiency through less time spent by staff on combating cybercrimes, with a more efficient product development, maintenance, and deployment environment achieved through vulnerability management.

c. Implementation of “Secure by Design” methodologies suggested by DHS/CISA.
d. Improved ability to manage your supply chain and vendors through licensing information found within metadata contained in SBOM/RBOM.
e. Updated and more efficient service engineering, development, production, support, maintenance, problem management, and recovery process life cycles.
f. Recognition and response to threat groups and sub-categories in adherence to modern techniques and procedures to proactively detect, respond to, and eliminate cyber-crimes, technology problems, and procedural flaws.

2. Improved awareness and training in cyber security incidents and technical problems.
a. Domestic and international efforts to combat cybercrimes and technical problems.
b. Software and hardware protection techniques identified and examined.
c. Awareness discussion on domestic and international laws and regulations.
d. Understanding of organizations critical products and services.
e. Problem / incident management procedures and component ownership definitions.
f. Business Continuity Management (BCM), Disaster Recovery(DR), and Continuity of Operations (**COOP**) to provide continuity of the business.
g. Learning Safeguards, detections, and responses to cybercrimes, technology threats and procedural flaws.

3. Vulnerability Risk Management Policy procedures guideline manual.
a. Business Analysis to define critical and most sensitive services, applications, and products.
b. Risk Assessment of current environment to uncover weaknesses and areas of improvement.
c. Audit review to define adherence to domestic and international laws and regulations.
d. Workflow analysis to define organizational workflow and identify areas for improvement through automation and streamline of functions.
e. Recommendations for improvement.
f. Plan and Implementation of desired improvements.
g. Organizational modification related to vulnerability management.
h. Awareness and Training for management, staff, and the public.

4. Vulnerability Management program product integration.
a. Product selection through implementation and integration guidelines and procedures.
b. Reduction in vulnerabilities through quicker identification, classification, and mitigation.
c. Automation processes develop and are integrated whenever possible.
d. Ongoing support and maintenance through a central group responsible for the Resilience Operation Center (ROC) and providing vulnerability advice throughout the organization.

5. DevSecOps and shift left in application testing processes deployed.
a. Code testing throughout the development and operations environments through Static, Dynamic, Interactive, and Runtime code evaluations.

   b. Vulnerability-free applications developed prior to production acceptance.
   c. Continuous Threat Exposure Management (**CTEM**) integration to identify and address threats before they can be exploited with Penetration Testing (PenTest), attack surface management (ASM), and Red-Teaming to ensure a proactive defense posture against cybercrimes and technical problems.

6. **Improved management and organization protection.**
   a. Adherence to laws and regulations.
   b. Improved staff loyalty, and
   c. Reduced toil and turnover due to burnout.
   d. Initiative-taking approach to resolving cyber-crimes, technology threats, and procedural flaws.

Where do we go from here?

If you found the information in this document valuable and want to learn more, or discuss implementing these procedures within your organization, then please contact me at:

Thomas Bronack, CBCP
bronackt@gmail.com
917-673-6992

I would love to hear about your needs and help you accomplish a more secure environment, with fewer costs consumed by cybersecurity and a happier staff.