Cyberator®

Are you cybersecure?

What is Cyberator?

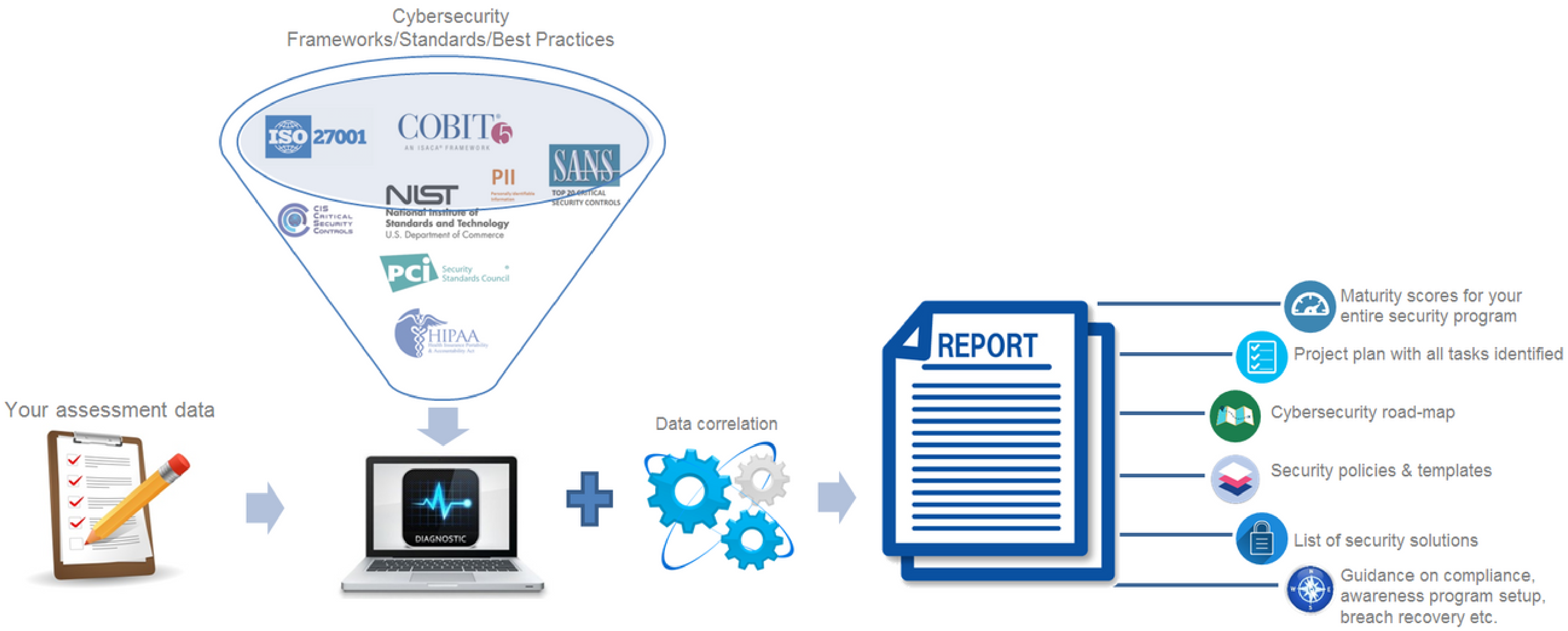
Cyberator is an all-in-one cybersecurity tool that simplifies the complexity of assessments, by leveraging its intelligence in merging and mapping cybersecurity frameworks against the existing and future posture of an organization. It provides automatic tracking of all gap remediation efforts, along with full control of road-map development, based on simple answers to a sophisticated tool that queries their environment.

With just 3 steps – completing the online self-assessment, reviewing the comprehensive report with our security expert and by taking the recommended actions, organizations can start their journey to become cyber secure in less than ½ a day that once required weeks to a month. The Return On Investment for using Cyberator is over 301%.

How does Cyberator work?

We've pre-built the **NIST** Cyber Security Framework**, ISO27001**, **SANS Top 20** Critical Security Controls, **CIS** Critical Security Controls and industry-specific regulations (**HIPAA**, **PII**, **PCI DSS**, **NERC CIP**, **FERC CIP**, **GLBA**, **FFIEC**, **FISMA**, and **SOX**) into questions for those on the front lines of your security enterprise.

Cyberator takes a 360 degree view of the organization's cybersecurity program in areas such as **process**, **people** and **technology**. As participants respond to predefined security questions, our analytics engine instantly measures each input's performance value using the five capability maturity model integration (**CMMI**) levels. Based on this data, it does a data correlation and computation to provide maturity scores for the entire cybersecurity program, along with a comprehensive improvement plan to address the gaps.



Cybersecurity Frameworks/Standards/Best Practices

Your assessment data

Data correlation

Maturity scores for your entire security program

Project plan with all tasks identified

Cybersecurity road-map

Security policies & templates

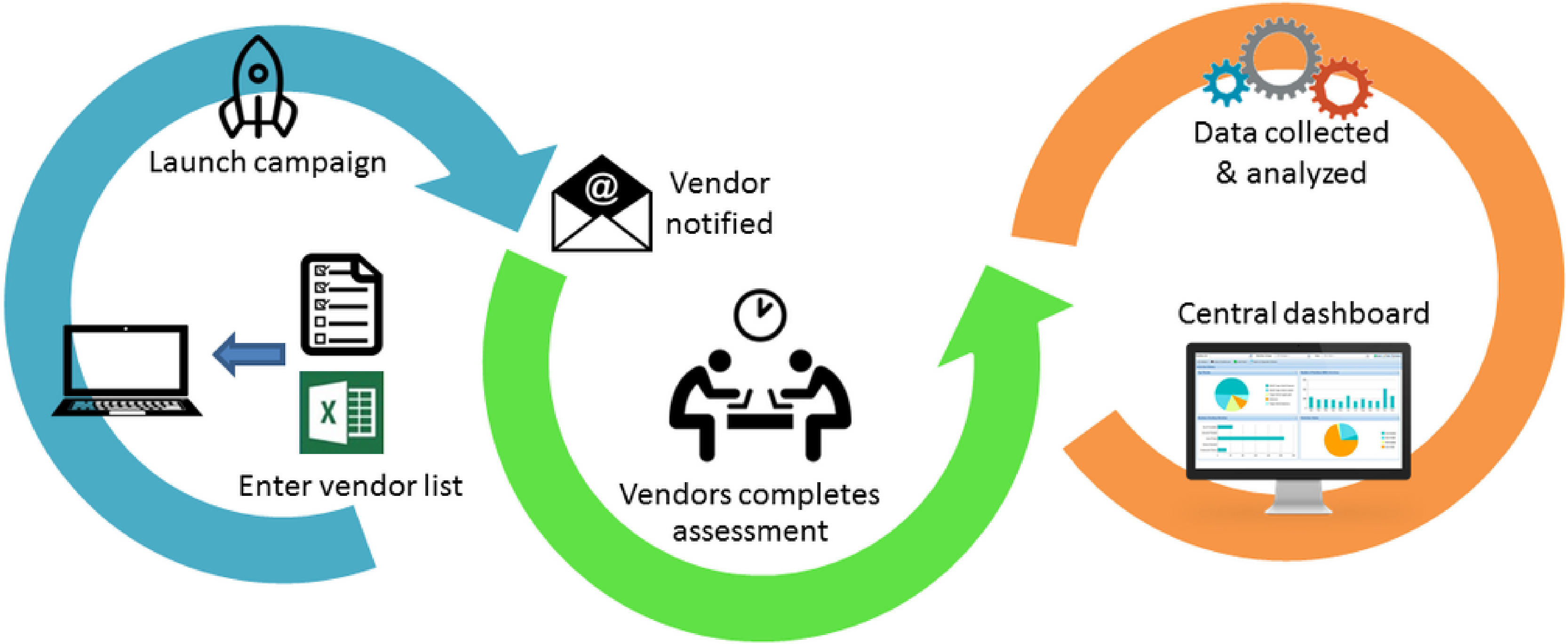
List of security solutions

Guidance on compliance, awareness program setup, breach recovery etc.

ISO 27001
COBIT 5
AN ISACA FRAMEWORK
PII
SANS
TOP 20 CRITICAL SECURITY CONTROLS
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
CIS Critical Security Controls
PCI Security Standards Council
HIPAA
DIAGNOSTIC
REPORT

Cyberator Streamlines 3rd party and IT risk audits with a centralized solution with minimal effort

Cyberator makes assessing or auditing your vendor, partner, supplier and other third-party relationships super easy. With just a few clicks, you can start automated campaigns for one or hundreds via the web console, collect the data and manage it using real-time dashboard. You can then view or print the reports for your on-site audit if needed.



Launch campaign

Vendor notified

Data collected & analyzed

Central dashboard

Enter vendor list

Vendors completes assessment

Offerings

Advisor Guided Implementation

+

The client completes his own assessment online.

Our security advisor will provide some guidance along the way on how to use the diagnostic tool to complete the self-assessment. We will also go over the scorecard and action plan with you and provide valuable advise. Up to 3 hours of phone consultation is included.

Subscription model

Unlimited use of the tool and can be used for multiple entities/3rd party assessments

+

The client completes his own assessment online.

Our security advisor will provide some guidance along the way on how to use the diagnostic tool to complete the self-assessment. We will also go over the scorecard and action plan with you and provide valuable advise.

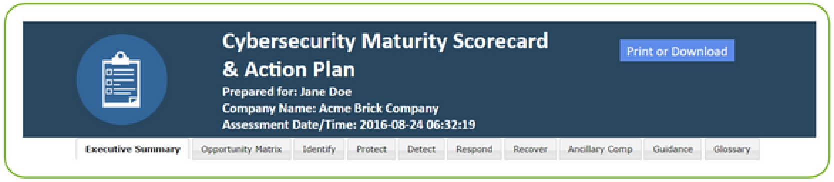
Consulting Service

On-site 5 Day Diagnostic Workshop

We will engage with you and help facilitate this Diagnostic program, interpret the results, and help you start to implement the change.

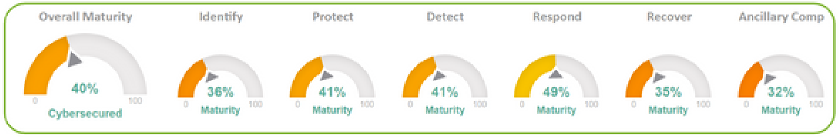
We take you through the phases of this process and ensure that you have a road map in place to improve the areas highlighted in your custom report.

Sample Reports



Cybersecurity Maturity Scorecard & Action Plan

Prepared for: Jane Doe
Company Name: Acme Brick Company
Assessment Date/Time: 2016-08-24 06:32:19



This Cybersecurity Maturity Scorecard grade is a comprehensive indicator of your relative cybersecurity health, or cybersecurity posture. Because only one vulnerable point in a security system is enough for a hacker or an attack to succeed, our Cybersecurity Maturity Scorecard takes a multidimensional approach to rating security.

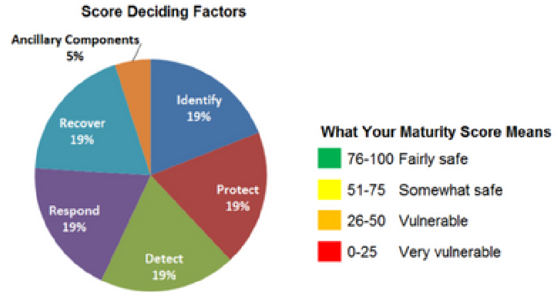
It's critical that the Cybersecurity practice addresses any weaknesses in the organization's functional structure (people and processes), before turning to technical products as potential solutions.

Cyber risk mitigation is a journey, not a destination. With each step in the process, the organization has an incrementally better cyber risk mitigation posture. As the cyber threat landscape changes - with new risks, new vulnerabilities, new businesses, the journey continues.

How to use this comprehensive report:

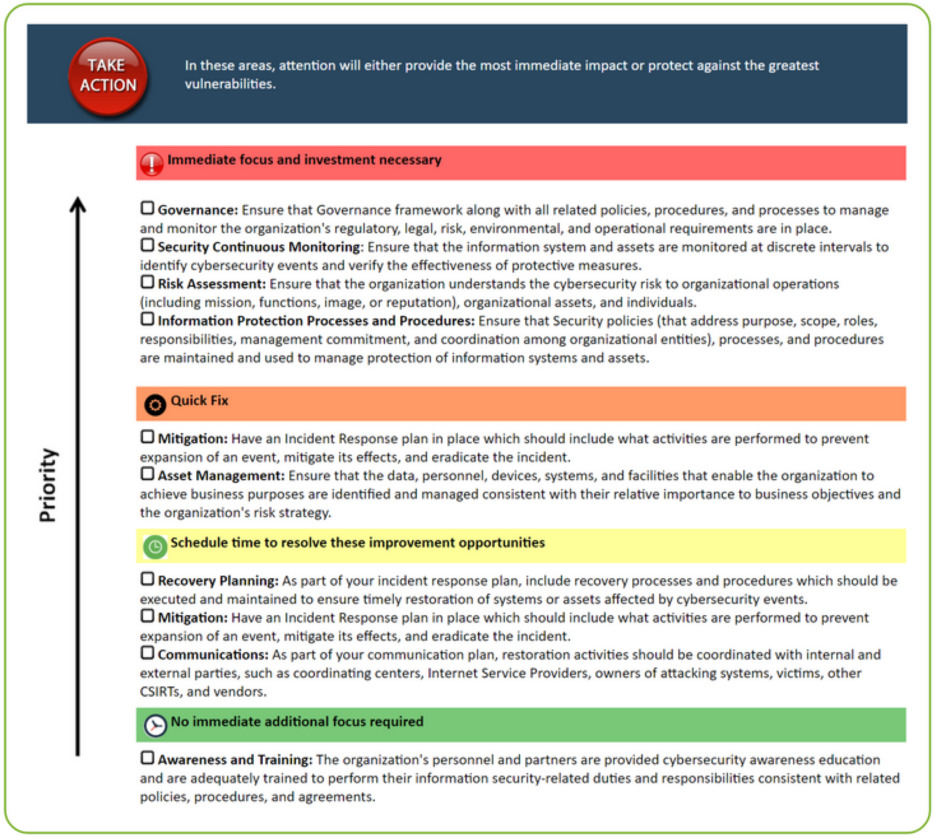
- We have done an assessment of the maturity of your current Cybersecurity Program based on your input and have identified areas for improvement. The report consists of 6 functional areas such as **Identify**, **Protect**, **Detect**, **Respond**, **Recover** and **Ancillary Components/ Initiatives**. Each has a prioritized roadmap for project investments and organizational change initiatives and you can view them by click on the tabs above. By addressing each of these action items, you should be able to get to your desired target state.

Maturity Scores: What you need to know



- We have also provided an opportunity matrix and indicated what areas need immediate attention.
- We have also provided links to valuable Resources, available Security Tools and Templates to aid you with your Cybersecurity program development.
- A Cybersecurity Glossary is included to help you familirize with the terms used in the cybersecurity space.

Areas Of Top Concerns/Initial Opportunity Matrix



In these areas, attention will either provide the most immediate impact or protect against the greatest vulnerabilities.

Immediate focus and investment necessary

□ **Governance:** Ensure that Governance framework along with all related policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are in place.
□ **Security Continuous Monitoring:** Ensure that the information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
□ **Risk Assessment:** Ensure that the organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
□ **Information Protection Processes and Procedures:** Ensure that Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Quick Fix

□ **Mitigation:** Have an Incident Response plan in place which should include what activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
□ **Asset Management:** Ensure that the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Schedule time to resolve these improvement opportunities

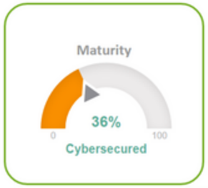
□ **Recovery Planning:** As part of your incident response plan, include recovery processes and procedures which should be executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
□ **Mitigation:** Have an Incident Response plan in place which should include what activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
□ **Communications:** As part of your communication plan, restoration activities should be coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

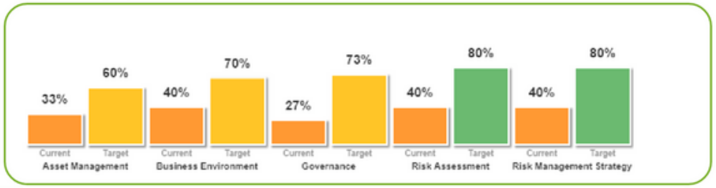
No immediate additional focus required

□ **Awareness and Training:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Function: Identify

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.





TAKE ACTION

For the **"Identify"** function, the organization, with guidance from the board or senior management, should develop the understanding to manage the cybersecurity risk to systems, assets, data, and capabilities. This would address issues such as risk assessment, asset management, and governance.

Based on the self-assessment you completed, we compared your Current Profile and the Target Profile to determine the gaps and provided you with the action plan below. Compare the list with the cybersecurity activities or controls that are currently either partially in place or not in place and develop a project plan. You would then prioritize this plan to address these gaps that draws upon your mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. You would then determine the resources necessary to address the gaps. For each identified activity or control, describe the way in which the organization does not meet the best practice in developing a Cybersecurity and Risk Mitigation Plan. You should make a note to either "Accept" or "Mitigate" the risk posed by not implementing the best practice. Assign a person or group responsible for mitigating or accepting the risk posed by not implementing the best practice. Provide an estimated completion date of mitigation in the "Estimated Completion Date" column of your project plan, or use "n/a" for risk acceptance. Describe the strategy that will be used to implement the activity or control, or use "n/a" for risk acceptance.

Using the Profiles in this manner will enable your organization to make informed decisions about cybersecurity activities, supports risk management, and enable the organization to perform cost-effective, targeted improvements. Take action to address the following:

☐ Have a Governance framework in place and approved at Board Level.Every organization needs to have a complete cybersecurity governance framework to fully address all of their cybersecurity needs. The key components that play crucial roles in shaping this security posture are:
1) Organizational structure;
2) Work culture;
3) Security awareness programs;
4)Cybersecurity governance.
Each of these aspects works with the others to cover gaps in security. While focusing on one specific area of need can make a difference, the most effective initiatives will use all four of these components to protect the organization.

☐ Have a cyber risk appetite statement approved by the board or an appropriate board committee.

☐ Have the risk to organization's information assets from a cyber attack as a regular agenda item for Board discussion.

☐ Create an overarching corporate information risk policy which is owned by the Board. This report contains links to sample policy templates that you can use.

☐ Adopted continuous through-life process to ensure security controls remain appropriate to risk.

☐ Apply recognised standards e.g. ISO27000 throughout the organization and implement physical, personnel, procedural and technical measures.

☐ Adapt risk management organization wide and driven by corporate governance from the top down.

☐ Information security risks should be discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.

☐ Implement an security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, and (5) is reliably monitored for employee completion.

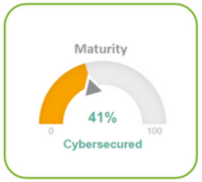
☐ Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.

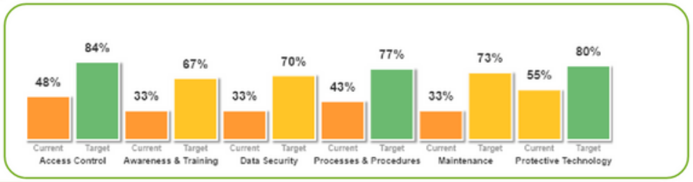
☐ Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery.

Back to top

Function: Protect

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.





TAKE ACTION

For the **"Protect"** function, develop and implement the appropriate safeguards to ensure delivery of services. This would include measures such as access control, data security, training, processes, and procedures.

Based on the self-assessment you completed, we compared your Current Profile and the Target Profile to determine the gaps and provided you with the action plan below for this function. Compare the list with the cybersecurity activities or controls that are currently either partially in place or not in place and develop a project plan. You would then prioritize this plan to address these gaps that draws upon your mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. You would then determine the resources necessary to address the gaps. For each identified activity or control, describe the way in which the organization does not meet the best practice in developing a Cybersecurity and Risk Mitigation Plan. You should make a note to either "Accept" or "Mitigate" the risk posed by not implementing the best practice. Assign a person or group responsible for mitigating or accepting the risk posed by not implementing the best practice. Provide an estimated completion date of mitigation in the "Estimated Completion Date" column of your project plan, or use "n/a" for risk acceptance. Describe the strategy that will be used to implement the activity or control, or use "n/a" for risk acceptance.

Using the Profiles in this manner will enable your organization to make informed decisions about cybersecurity activities, supports risk management, and enable the organization to perform cost-effective, targeted improvements. Take action to address the following:

☐ Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

☐ Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.

☐ Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.

☐ Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

☐ Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

☐ Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

☐ Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively [illegible]

☐ Assign job titles and duties for handling computer and network incidents to specific individuals.

☐ Define management personnel who will support the incident handling process by acting in key decision-making roles.

☐ Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).

☐ Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.

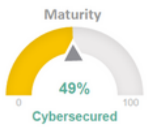
☐ Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

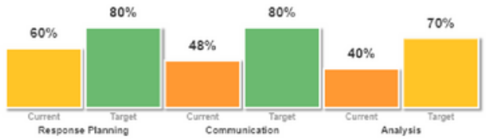
☐ Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outsi

Back to top

Function: Respond

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.





TAKE ACTION

For the **"Respond"** function, develop and carry out the appropriate actions to take once a cybersecurity event is underway. These include response planning, communications, analysis, mitigation, and other improvements.

Based on the self-assessment you completed, we compared your Current Profile and the Target Profile to determine the gaps and provided you with the action plan below for this function. Compare the list with the cybersecurity activities or controls that are currently either partially in place or not in place and develop a project plan. You would then prioritize this plan to address these gaps that draws upon your mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. You would then determine the resources necessary to address the gaps. For each identified activity or control, describe the way in which the organization does not meet the best practice in developing a Cybersecurity and Risk Mitigation Plan. You should make a note to either "Accept" or "Mitigate" the risk posed by not implementing the best practice. Assign a person or group responsible for mitigating or accepting the risk posed by not implementing the best practice. Provide an estimated completion date of mitigation in the "Estimated Completion Date" column of your project plan, or use "n/a" for risk acceptance. Describe the strategy that will be used to implement the activity or control, or use "n/a" for risk acceptance.

Using the Profiles in this manner will enable your organization to make informed decisions about cybersecurity activities, supports risk management, and enable the organization to perform cost-effective, targeted improvements. Take action to address the following:

□ Appropriate steps should be taken to contain and control an incident to prevent further unauthorized access to or use of customer information.

□ The incident response plan should be designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.

□ Have a process is in place to help contain incidents and restore operations with minimal service disruption.

□ Develop containment and mitigation strategies for multiple incident types (e.g., DDoS, malware).

□ Develop procedures for containment strategies and notifying potentially impacted third parties.

□ Develop processes to trigger the incident response program when an incident occurs at a third party.

□ Develop capabilities to generate reports to support incident investigation and mitigation.

□ Setup contracts and relationship with third parties so that you can call upon them, as needed, to provide mitigation services.

□ Setup regular task to perform analysis of events to improve the institution's security measures and policies.

□ Analysis of security incidents should be performed in the early stages of an intrusion to minimize the impact of the incident.

□ Any changes to systems/applications or to access entitlements necessary for incident management should be reviewed by management

□ Develop your organization's risk management plan so that significant cyber incidents should result in limited to no disruptions to critical services.

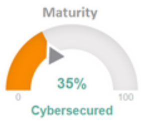
□ Engineer your technology infrastructure to limit the effects of a cyber attack on the production environment from migrating to the backup environment (e.g., air-gapped environment and processes).

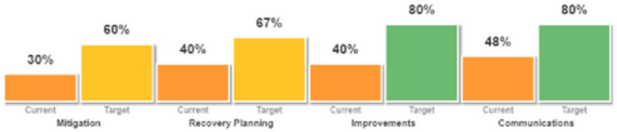
□ Focus sharing on actionable threat, vulnerability, and mitigation information: Shared threat, vulnerability, and mitigation information can create immediate improvements in cybersecurity and can help create better outcomes for ICT consumers in general. Sharing actionable information empowers actors to better defend networks and mitigate threats. Exchanging this type of data can help to build trust particularly in early stages of information sharing. Automated sharing mechanisms are increasingly used to rapidly share and act upon this information. Using machine readable formats to exchange threat and mitigation information can help automate defenses and reduce risk.

Back to top

Function: Recover

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.





TAKE ACTION

For the **"Recover"** function, develop and carry out the appropriate activities to restore any capabilities or services that were impaired due to a cybersecurity event. The focus should be to maintain resilience for the network and protect it from further attacks.

Based on the self-assessment you completed, we compared your Current Profile and the Target Profile to determine the gaps and provided you with the action plan below for this function. Compare the list with the cybersecurity activities or controls that are currently either partially in place or not in place and develop a project plan. You would then prioritize this plan to address these gaps that draws upon your mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. You would then determine the resources necessary to address the gaps. For each identified activity or control, describe the way in which the organization does not meet the best practice in developing a Cybersecurity and Risk Mitigation Plan. You should make a note to either "Accept" or "Mitigate" the risk posed by not implementing the best practice. Assign a person or group responsible for mitigating or accepting the risk posed by not implementing the best practice. Provide an estimated completion date of mitigation in the "Estimated Completion Date" column of your project plan, or use "n/a" for risk acceptance. Describe the strategy that will be used to implement the activity or control, or use "n/a" for risk acceptance.

Using the Profiles in this manner will enable your organization to make informed decisions about cybersecurity activities, supports risk management, and enable the organization to perform cost-effective, targeted improvements. Take action to address the following:

□ Conducting analyses on cybersecurity incidents: A greater understanding of the root causes of cybersecurity incidents can help prevent future incidents and can foster improved security analyses. In many cases, a detailed analysis of the incidents can inform the selection and prioritization of cybersecurity risk mitigations for your organization and can also help build knowledge of long-term trends, giving network defenders a better understanding of emerging cyber-threats and of shifts in exploitation methods.

□ Require mandatory information sharing only in limited circumstances. Mandatory incident reporting is very different than voluntary information sharing. In some instances, such as in the case of national security and public safety, there may be a need for mandatory incident reporting. But such mandatory approaches should be narrowly defined and implemented through trusted mechanisms. This helps ensure that only the right information is shared with the appropriate stakeholders in the proper timeframe. Moreover, such a narrow approach strengthens privacy and the protection of civil liberties. Policy efforts should encourage information sharing processes, which are transparent about how such data is used and which ensure that information shared back to the submitters is valuable and timely.

□ Incorporate lessons learned from real-life cyber incidents and attacks on the institution and other organizations to improve the organization's risk mitigation capabilities and response plan.

□ Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

□ Establish methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans.

Back to top

Guidance

Common Regulatory Obligations

For better or worse, IT is in the spotlight with regard to compliance. Suddenly, IT departments everywhere have been charged by the CEO, CFO, and Audit Committee with making the company compliant, because many of the laws carry personal liability penalties for officers and directors of corporations. Depending on the industry you are in, your organization may be used to regulations or completely new to them. At the heart of most regulations is the intention of protecting the confidentiality, integrity, and availability of information that impacts a corporation's stakeholders. These laws can be distilled down to there essential goals:

- Establish and implement controls
- Maintain, protect, and assess compliance issues
- Identify and remediate vulnerabilities and deviations
- Provide reporting that can prove your organization's compliance

Here's a quick look at the laws and regulations that have immediate impact on your organization and cybersecurity, in just enough detail to understand what each law is about. But don't assume this list represents all of the laws and regulations that may apply to your business.

Sarbanes Oxley Act (SOX)
Applies to public companies that have registered equity or debt securities within the SEC to guarantee data integrity against financial fraud
Who is affected: U.S. public company boards management and public accounting firms.

Payment Card Industry Data Security Standard (PCI-DSS)
Applies to any organization that processes transmits or stores credit card information to ensure cardholder data is protected
Who is affected: Retailers credit card companies anyone handling credit card data.

Security Breach Notification Laws
Most US states have specific Security Breach Notification Laws - please review them for the state(s) your organization has office(s) in.

Personal Information Protection and Electronic Documents Act (PIPEDA)
Applies to private sector organizations that collect personal information in Canada to ensure the protection of personal information in the course of commercial business

Be Ready With Your Answers

Increasingly, cybersecurity is becoming a top-of-mind issue for most CEOs and boards due to increased pressure from government regulators and shareholders, and they are becoming more preemptive in evaluating cybersecurity risk exposure as an enterprisewide risk management issue, not limiting it to an IT concern. Here are some questions a CISO is likely to face when presenting to the board or the CxO:

Key Questions the Board May Ask Cybersecurity Chiefs:

- What was our most significant cybersecurity incident in the past quarter? What was our response?
- What is our maturity level in cybersecurity?
- How quickly can we react when a breach takes place?
- Do we have enough visibility into our possible vulnerabilities?
- How much will it cost us if we are breached?
- Do we have the right talent and resources? How much will it cost us to get there?
- How is the performance of the security team evaluated?
- What was our most significant near miss? How was it discovered?
- Do you have relatioonships with law enforcement, such as the FBI and Interpol?
- Do you work with business leaders on due diligence of acquisition targets? With supply chain leaders on security protocols of vendors and other partners?
- What process is in place to ensure you can escalate serious issues and provide prompt, full disclosure of cybersecurity deficiencies?

Questions you can expect from the CxO :

- What do you need from my division to help with the cybersecurity efforts?
- Could you show us the breakdown of investments in the cybersecurity sector? How are you determining how to invest on what?
- What impact will customers notice as improvements are made in cybersecurity?
- How will the daily transactions be affected by improvements in cybersecurity?
- What can be advertised about improvements?

Steps to take after a breach

Recommended Steps You Should Take After A Data Breach:

As demonstrated by recent security breaches of several large, tech-savvy companies, no set of security measures is completely infallible to a breach. What businesses of today have to then consider is: what is your plan of action after a data breach when your security and data loss prevention measures have failed? Effective response to a data breach can mean the difference between minimized impact and closing your doors for good.

Here are some best practices to apply after a data breach has already occurred:
Step one: Follow, turn-by-turn, the organization's incident response plan. This, of course, presupposes that such a plan is both extant and well done.

Ensure that your systems are out of danger. Call in your team of network security experts to assess the breach, identify the source of the breach and contain the damage. It is vital to identify the compromised system in the shortest possible time and fix the data leak to prevent future attacks.

Understand the root of the issue. Engineers can use forensics to analyze traffic and instantly determine the root cause of an event, entirely removing guesswork and problem reproduction from the equation. Effective forensics provide these four key capabilities:

- Data Capture: Capture all traffic, 24x7, on even the fastest links
- Network Recording: Store all packets for post-incident, or forensic analysis
- Search and Inspection: Enable administrators to comb through archived traffic for anomalies and signs of problems
- Reporting: Through data capture and analysis, results of investigations are logged and network vulnerabilities are reviewed and analyzed post-mortem.

Perhaps most importantly, forensics solutions capture data 24/7 and automatically analyze all data collected in real time, which means all the data you need for analysis is available at a moment's notice. Whether the problem with your mission-critical app is across the room or across the world, forensics gives you immediate access to the most detailed analytics available to get to the root cause of an issue. If an incident response plan does not exist, has not been tested, and/or is not well crafted at your organization, then the first step is quite different which is to bring in a third-party IT professional that specializes in incident response and gap analysis.

Step two: Contact your legal representative to ensure your response meets all legal requirements. You want to avoid being personally liable for damage resulting from a data breach at your organization. Your response may include internal investigation, contacting law enforcement, complying with mediation and notification requirements, and planning a public-relations strategy.

Step three: Notify. Research your state's law on whom to notify in case of a breach (sometimes the data subjects, sometimes a government agency), see whether your breach fits the type covered by the law; then check the 4-5 federal laws requiring notification in the event of CERTAIN breaches. Some states require written notification of data breaches, and most call for identification of the specific information that was exposed in the breach. Note that California's breach-notification statute was recently expanded to broaden the definition of personally identifiable information. Particularly thorny for tech startups are the notification statute's "reasonable belief" and "unreasonable delay" requirements. The uncertainty about what constitutes a failure to inform has the potential of increasing liability for companies hit by a data breach. Forty-seven states and the District of Columbia require organizations requires you to notify customers and clients when their personal information has been stolen. Publicly traded companies are subject to SEC reporting guidelines about data theft and other crimes. If companies fail to protect customer data appropriately, they may be subject to Federal Trade Commission scrutiny for violating their own privacy policies.

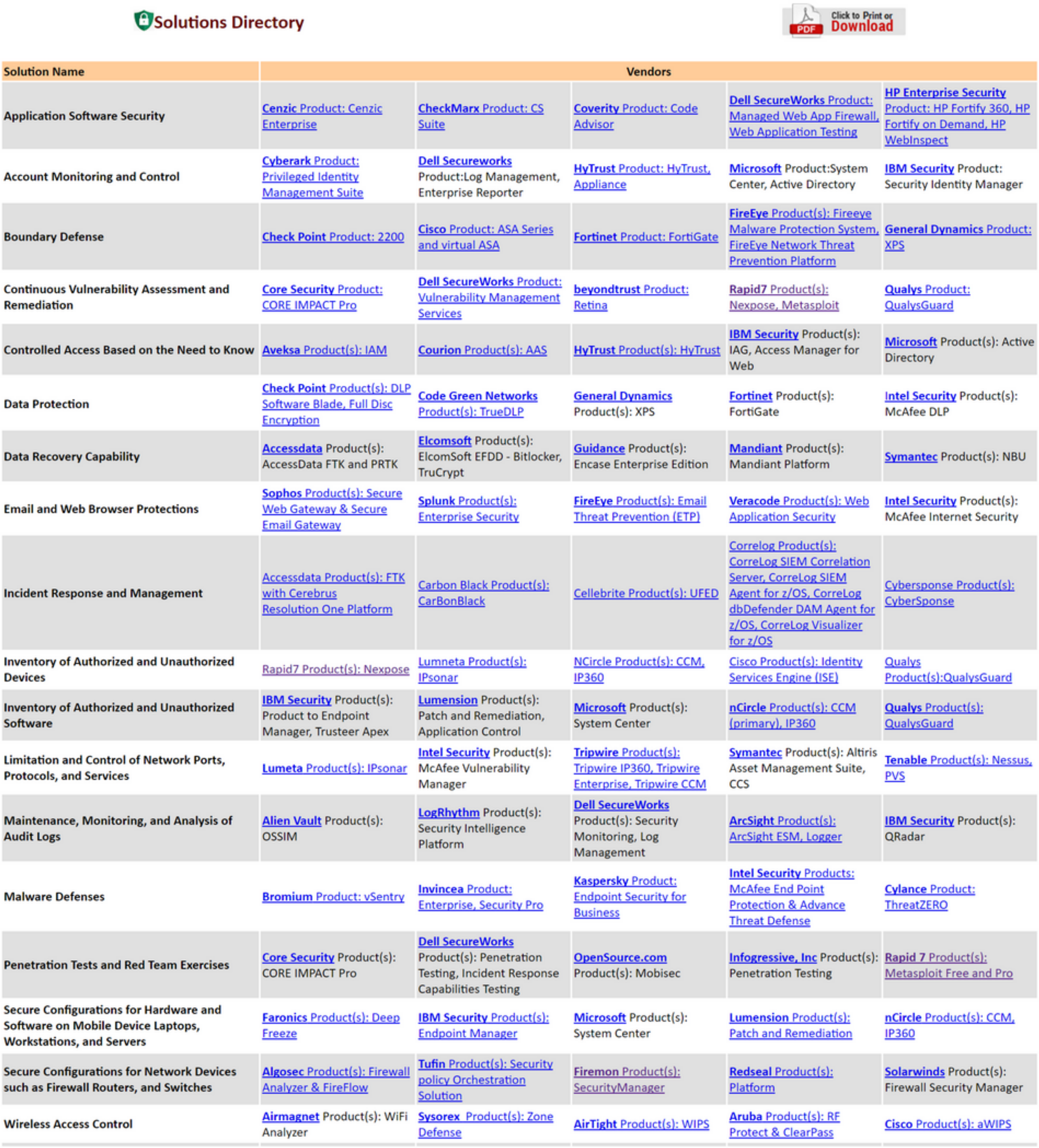
Most important in this step is developing a single voice message about the breach for potential victims, employees, and the media. A firm's best chance of survival after a breach is to limit rumors and enhance trust. Your notification and all other communications with the public about the breach should emphasize the company's willingness to make things right and to prevent future breaches. Take ownership of the problem, but include only the information required by law. Be sure to keep the notification short and simple.

Step four: Check your insurance coverage. Your company's comprehensive general liability (CGL) policy may cover invasion of privacy claims related to the breach, absent an explicit exclusion for threats like phishing attacks and cyber-attacks and resulting data breaches. However, the trend is toward purchasing cyber insurance as a separate policy. Consider whether your main concerns are identity theft, loss of trade secrets, breach of confidentiality agreements, or some combination thereof. Then perform a cost-benefit analysis of how likely those losses are and what they will cost you. Then negotiate appropriate cyber coverage and be acutely aware what is covered in your policy, in your cloud provider's policy and your counterparties' policies. When the time comes and the breach occurs, immediate notification of your carrier and insurance broker is essential. Then, in conjunction with your broker and in-house and outside attorneys, ride herd on the carrier to make sure it provides what it bargained for.

Step five: Do a post-mortem. Last but not least, re-examine your security measures to determine what action you can take to prevent being damaged by a similar attack in the future.

Back to top

A list of security products to help you implement the Critical Security Controls

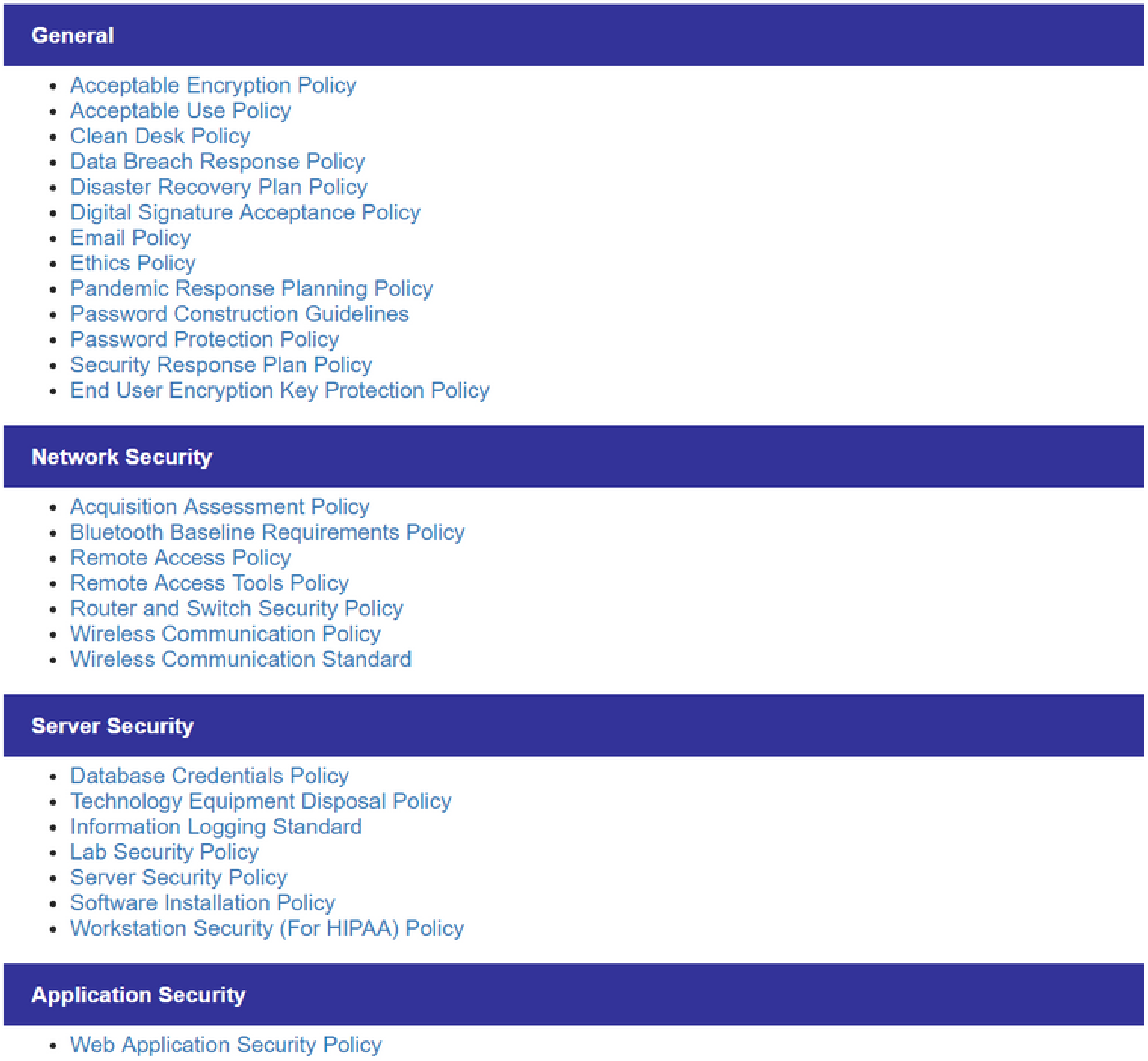


Solutions Directory

Click to Print or Download

Solution Name	Vendors				
Application Software Security	Cenzic Product: Cenzic Enterprise	CheckMarx Product: CS Suite	Coverity Product: Code Advisor	Dell SecureWorks Product: Managed Web App Firewall, Web Application Testing	HP Enterprise Security Product: HP Fortify 360, HP Fortify on Demand, HP WebInspect
Account Monitoring and Control	Cyberark Product: Privileged Identity Management Suite	Dell Secureworks Product:Log Management, Enterprise Reporter	HyTrust Product: HyTrust, Appliance	Microsoft Product:System Center, Active Directory	IBM Security Product: Security Identity Manager
Boundary Defense	Check Point Product: 2200	Cisco Product: ASA Series and virtual ASA	Fortinet Product: FortiGate	FireEye Product(s): Fireeye Malware Protection System, FireEye Network Threat Prevention Platform	General Dynamics Product: XPS
Continuous Vulnerability Assessment and Remediation	Core Security Product: CORE IMPACT Pro	Dell SecureWorks Product: Vulnerability Management Services	beyondtrust Product: Retina	Rapid7 Product(s): Nexpose, Metasploit	Qualys Product: QualysGuard
Controlled Access Based on the Need to Know	Aveksa Product(s): IAM	Courion Product(s): AAS	HyTrust Product(s): HyTrust	IBM Security Product(s): IAG, Access Manager for Web	Microsoft Product(s): Active Directory
Data Protection	Check Point Product(s): DLP Software Blade, Full Disc Encryption	Code Green Networks Product(s): TrueDLP	General Dynamics Product(s): XPS	Fortinet Product(s): FortiGate	Intel Security Product(s): McAfee DLP
Data Recovery Capability	Accessdata Product(s): AccessData FTK and PRTK	Elcomsoft Product(s): ElcomSoft EFDD - Bitlocker, TruCrypt	Guidance Product(s): Encase Enterprise Edition	Mandiant Product(s): Mandiant Platform	Symantec Product(s): NBU
Email and Web Browser Protections	Sophos Product(s): Secure Web Gateway & Secure Email Gateway	Splunk Product(s): Enterprise Security	FireEye Product(s): Email Threat Prevention (ETP)	Veracode Product(s): Web Application Security	Intel Security Product(s): McAfee Internet Security
Incident Response and Management	Accessdata Product(s): FTK with Cerebrus Resolution One Platform	Carbon Black Product(s): CarBonBlack	Cellebrite Product(s): UFED	Correlog Product(s): CorreLog SIEM Correlation Server, CorreLog SIEM Agent for z/OS, CorreLog dbDefender DAM Agent for z/OS, CorreLog Visualizer for z/OS	Cybersponse Product(s): CyberSponse
Inventory of Authorized and Unauthorized Devices	Rapid7 Product(s): Nexpose	Lumneta Product(s): IPsonar	NCircle Product(s): CCM, IP360	Cisco Product(s): Identity Services Engine (ISE)	Qualys Product(s):QualysGuard
Inventory of Authorized and Unauthorized Software	IBM Security Product(s): Product to Endpoint Manager, Trusteer Apex	Lumension Product(s): Patch and Remediation, Application Control	Microsoft Product(s): System Center	nCircle Product(s): CCM (primary), IP360	Qualys Product(s): QualysGuard
Limitation and Control of Network Ports, Protocols, and Services	Lumeta Product(s): IPsonar	Intel Security Product(s): McAfee Vulnerability Manager	Tripwire Product(s): Tripwire IP360, Tripwire Enterprise, Tripwire CCM	Symantec Product(s): Altiris Asset Management Suite, CCS	Tenable Product(s): Nessus, PVS
Maintenance, Monitoring, and Analysis of Audit Logs	Alien Vault Product(s): OSSIM	LogRhythm Product(s): Security Intelligence Platform	Dell SecureWorks Product(s): Security Monitoring, Log Management	ArcSight Product(s): ArcSight ESM, Logger	IBM Security Product(s): QRadar
Malware Defenses	Bromium Product: vSentry	Invincea Product: Enterprise, Security Pro	Kaspersky Product: Endpoint Security for Business	Intel Security Products: McAfee End Point Protection & Advance Threat Defense	Cylance Product: ThreatZERO
Penetration Tests and Red Team Exercises	Core Security Product(s): CORE IMPACT Pro	Dell SecureWorks Product(s): Penetration Testing, Incident Response Capabilities Testing	OpenSource.com Product(s): Mobisec	Infogressive, Inc Product(s): Penetration Testing	Rapid 7 Product(s): Metasploit Free and Pro
Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers	Faronics Product(s): Deep Freeze	IBM Security Product(s): Endpoint Manager	Microsoft Product(s): System Center	Lumension Product(s): Patch and Remediation	nCircle Product(s): CCM, IP360
Secure Configurations for Network Devices such as Firewall Routers, and Switches	Algosec Product(s): Firewall Analyzer & FireFlow	Tufin Product(s): Security policy Orchestration Solution	Firemon Product(s): SecurityManager	Redseal Product(s): Platform	Solarwinds Product(s): Firewall Security Manager
Wireless Access Control	Airmagnet Product(s): WiFi Analyzer	Sysorex Product(s): Zone Defense	AirTight Product(s): WIPS	Aruba Product(s): RF Protect & ClearPass	Cisco Product(s): aWIPS

Security Policy Templates available for download



General

- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Data Breach Response Policy
- Disaster Recovery Plan Policy
- Digital Signature Acceptance Policy
- Email Policy
- Ethics Policy
- Pandemic Response Planning Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy
- End User Encryption Key Protection Policy

Network Security

- Acquisition Assessment Policy
- Bluetooth Baseline Requirements Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Wireless Communication Policy
- Wireless Communication Standard

Server Security

- Database Credentials Policy
- Technology Equipment Disposal Policy
- Information Logging Standard
- Lab Security Policy
- Server Security Policy
- Software Installation Policy
- Workstation Security (For HIPAA) Policy

Application Security

- Web Application Security Policy