Cybersecurity Program Checklist

Recommended Best Practices to Strengthen a Security Program

The following checklist is a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. It is by no means a comprehensive list, nor a guarantee that your organization will not be breached. This list is intended to help strengthen, prioritize, and focus on a smaller number of actions with high pay-off results.

Incident Response Capability

Help your organization deal quickly and efficiently with security incidents to reduce their impact.

- □ Executive support with clear ownership
- □ Form a Cybersecurity Emergency Response Team (CERT) with clearly defined roles
- □ Create your Cybersecurity incident response plan (CSIRP)
- □ Test your plan regularly with tabletop exercises

Security Awareness Training

Decrease the opportunity for compromise with regular training on social engineering methods attackers are using today.

- □ Implement a program for security awareness training and track compliance at all employee levels
- □ Consider social engineering tests as part of the security awareness program

Cyber Risk Management

Through self-audit or third party services, identify areas of needed improvement and prioritize improvement actions.

- □ At least annually, conduct a cyber risk assessment, utilizing a standard such as NIST, to identify cyber risks within the infrastructure
- □ Prioritize identified risks based on budget and resources, critical infrastructure, critical services, and critical data
- □ Develop plan for risk mitigation or risk transfer based on identified risks and priorities

Conduct Regular Inventory

Be aware of every device that is connected to your infrastructure and every piece of software and their purpose.

- □ Identify and remove unauthorized assets and software
- □ Prioritize critical assets and applications based on function and stored data
- □ Update CSIRP, network security architecture, and other elements of the program based on inventory results

Get Started Today

Contact us today to take advantage of these services and improve your organization's protection against a cyber attack:

- Visit www.aig.com/CyberRiskConsulting and complete the contact form, or
- Email us at CyberRiskConsulting@aig.com

Vulnerability Management

Eliminate known exposures in your infrastructure with regular vulnerability scanning and remediation efforts.

- □ Executive support with clear ownership
- □ Define a process for tracking and conducting remediation of identified vulnerabilities
- □ If you develop your own applications, conduct secure code evaluations prior to production launch of developed code

Proactive Security Testing

Security compliance is not enough. Proactively test your environment and eliminate further exposures.

- □ At least annually, conduct external penetration testing on applications and all publically exposed systems
- □ At least annually, conduct internal penetration testing on all systems and user end points
- □ Consider red team exercises to test critical systems, security processes, and personnel response

Patch Management

Keep your systems from becoming an easy target by maintaining the latest levels of software.

- □ Inventory and track all current versions of operating systems and other software installed in your environment
- □ Define a process designating resources and methodology to ensure timely application of patches to all systems in your infrastructure

Network Security Architecture

Protect your IT infrastructure and reduce the risks of breaches by limiting the damage of a successful attack.

- □ Identify most critical assets and data and separate them with network segmentation and strict access control
- □ Implement further segmentation to add layers of protection to your infrastructure
- □ Map network data flow and implement firewall and router rule sets to eliminate unnecessary data routes in the network

Network Security Principles

Take steps to reduce the attack surface in your IT environment and more quickly identify threats.

- □ Regularly audit firewall and router rule sets and remove default admin passwords
- □ Eliminate unnecessary services and unused ports
- □ Implement logging and maintain at least 30 days history for all network devices and systems
- □ Implement 24x7 security monitoring
- □ Consider implementing DDoS protection with a third party service
- □ Consider a strategy for end to end encryption protection of your data including cloud services

Identity and Access Control

Ensure the right individuals access the right resources at the right times and for the right reasons.

- □ Define and implement a strong user password policy requiring regular password changes
- □ Classify data and systems and define user roles utilizing least privilege model
- □ Take steps to eliminate or secure shared administrator accounts
- □ Monitor privileged user account activity for inappropriate behavior

User Security Policy

Define policy to protect your IT environment and manage endpoints such as laptops, tablets, and smart phones that access your network.

- □ Define and implement secure configuration policy eliminating unnecessary services or high risk actions like bit torrent file sharing services
- □ Install anti-virus software and conduct regular scans
- □ Scan guest and employee systems for malware and other risks before network access is given
- □ Require whole disk encryption on any device accessing company data

Data Recovery Capability

Eliminate the need to pay ransoms and further protect your business from data loss.

- □ Define and implement a policy for data backup and recovery including any cloud provider service
- □ Utilize tools to automate regular backups of identified critical data
- □ Ensure backups are not directly connected to your network and safely locked away
- □ Regularly test data recoverability from backups to ensure an efficient process that works
- □ Ensure your data recovery plan is tied to your incident response plan

Secure Supply Chain

Monitor the security of third party devices and services involved in your business to eliminate the introduction of security flaws from your partners.

- □ Monitor the security of third party organizations you work with via a security rating service
- □ Conduct security testing on third party devices and software utilized in your business and products
- □ Test and request proof of cloud and other service providers of security measures taken to protect your data and business
- □ Implement contractual language to hold third parties accountable

AIG®

Get Started Today

- Visit www.aig.com/CyberRiskConsulting and complete the contact form, or
- Email us at CyberRiskConsulting@aig.com

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG's core businesses include Commercial Insurance and Consumer Insurance, as well as Other Operations. Commercial Insurance comprises two modules – Liability and Financial Lines, and Property and Special Risks. Consumer Insurance comprises four modules – Individual Retirement, Group Retirement, Life Insurance and Personal Insurance. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange. Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this press release. AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.© American International Group, Inc. All rights reserved.

06/17