CYBERSECURITY PREPARATION CHECKLIST

Four Steps to Prepare for and Defend Against an Imminent Attack

The practices below can help reduce both the likelihood of a cyber attack and the impact should one occur. Please reference this checklist as a reminder to continue strengthening cyber resiliency and hardening infrastructure.

Step 1: Review Existing Defense Capabilities

Examine existing cybersecurity defense capabilities to determine critical gaps so improvements can be made to prepare for and better defend against a potential attack.

a. Review security intelligence and news sources to determine what security capabilities the target may use against you.
b. Review the security controls you have in place, including, but not limited to:
   i. Perimeter protection, e.g. firewalls, IDPS or anti-DDoS;
   ii. Anti-malware;
   iii. Critical asset (physical, digital) monitoring, e.g. DLP;
   iv. Events/logs monitoring; and
   v. Incident reporting and response capabilities.
c. Review any security services provided by outsourced provider(s) or partner(s).
d. Identify potential gaps in current controls against possible attack types.

Step 2: Verify Functionality and Currency

Strengthen cybersecurity hygiene and reduce gaps in current capabilities where possible.

a. Check that all security devices[1] are online and performing. This includes reporting logs, if applicable.
b. Address any at-capacity or configuration concerns on security devices.
c. Ensure all devices that may be involved in an attack are updated with the most current patches and firmware.
d. Run a vulnerability scan against your assets to identify any critical vulnerabilities or unnecessary open ports that could be exploited. Work to remediate them.
e. Ensure anti-virus, IPS or other signature-based detection systems are current with the latest updates.
f. Obtain the latest asset inventory, including company approved, BYOD, contractor and third-party devices. Determine if any involved hardware is aged or sunset and consider actions to remove, harden or protect it.
g. Review all user IDs and remove any IDs that are no longer in use or necessary.
h. Establish that every critical system and application can be restored from scratch if necessary.
i. Make sure you have current backups that are offline and in protected areas from an attack and that they have been tested for restore capabilities.
j. Determine if there are any third-party service providers that you need to coordinate with in the event of a potential attack and put them on alert for quick response, if needed.

If your environment contains critical infrastructure, such as SCADA or IoT controls for utilities or manufacturing:

k. Ensure no device is directly connected to the internet that does not have to be.
l. Increase the monitoring of traffic and alerts to and from these systems.
m. Ensure security controls in these environments are up to date.
n. Remind engineers to not connect personal devices to any SCADA or industrial control systems.

Step 3: Establish a Baseline for Anomaly Detection

If anomaly-based cybersecurity controls are in place, review the current baseline activity and ensure active monitoring is ready to help uncover any related indicators of compromise from a potential attack that may not be detected by signature-based security controls.

a. Review normal network traffic activity and patterns to establish a baseline based on business locations, time of day, ports, destinations and more.
b. Be prepared to flag any traffic that is suspicious or not part of the normal pattern, to normal countries or at normal times.
c. Test for the presence of deviations from standard internal or external traffic patterns to improve the ability to quickly detect change.
d. Ensure staff can pivot to detect new types of traffic traversing both internal networks as well as traffic ingress and egress to hosts on the DMZ.
e. Ensure logging is enabled on all critical systems and for all activities, e.g. new user account creation.
f. Temporarily turn off or limit non-essential services to reduce attack surface and exposure to the internet.

Step 4: Increase Organizational Awareness Through Employee Communications

Employees are an organization's most critical cybersecurity defense asset. Notify employees of potential threats and remind them of incident reporting procedures.

a. Distribute a notification (or multiple) to all employees advising them to be on high alert and to watch out for phishing and social engineering attacks. Notifications may include reminders such as:
   i. Click with care. Do not click links or attachments in an email that seem suspicious.
   ii. Sound the phishing email alarm. Report any suspected potential phishing emails.
   iii. Deny unusual requests. Beware of any email from a senior executive that includes an atypical request.
   iv. Do not give access to strangers. Do not trust someone who calls unexpectedly and demands access to your computer.
   v. Think before you upload or download. Remember that removable storage devices (e.g. flash drives) can be unsafe. Be certain that any software you intend to download is from a trusted source.
b. If using a security awareness training platform, have all employees complete short training modules to refresh their knowledge.
c. Communicate with executive staff on the imminent threat of an attack and ensure executive support for preparation and response activities.
d. Communicate with all IT and IT security staff. Make sure they are on high alert and consider increased staffing levels for timely identification and quick response to any issues.
e. Communicate with the help desk. Make sure they are on high alert and bring to your attention anything out of the ordinary or increased levels of activity or calls.

For additional help, email cyberriskconsulting@aig.com.

[1] Security device refers to any device deployed in the client's network that can be used to detect and/or protect them from an incoming attack.

This document is for general informational purposes only, and has been compiled from sources believed to be reliable. AIG accepts no legal responsibility for the correctness or completeness of this material or its application to specific factual situations. Reliance upon, or compliance with, any recommendation herein in no way guarantees any result, including without limitation the fulfillment of your obligations under your insurance policy or as may otherwise be required by any laws, rules or regulations. No responsibility is assumed for the discovery and/or elimination of any hazards that could cause accidents, injury or damage. This document should not be construed as financial, accounting, tax or legal advice and does not create an attorney-client relationship.

American International Group, Inc. (AIG) is a leading global insurance organization. Building on 100 years of experience, 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 common stock is listed on the New York Stock Exchange. Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. 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 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.