Cyber Resiliency Tips

The global impact of recent major ransomware events has highlighted both the increasing threat from failures of cyber security and the importance of IT systems to every facet of business. This note is intended to remind and reinforce those practices which create cyber resiliency. This note is not a comprehensive review of recent outbreaks; that information is readily available through other sources.

There are no silver bullets to cyber risk, but the below good practices will reduce both the likelihood of an event and the severity should one occur.

What Can Your Organization Do?

- **Inventory all systems** in your environment, paying special attention to identify end of life systems. Migrate to more current and in-support versions as soon as practical, and make sure the risk is understood and additional compensating controls are employed until migration can take place. Do not rely on older, out-of-date products for the most critical applications and data access.
- **Make patching systems** in a regular and timely fashion a priority. The great majority of malicious programs (malware) leverage known vulnerabilities in operating systems or applications for which patches are available. Not updating means these systems remain vulnerable.
- **Externally scan** the environment, paying special attention to services and open ports. Attackers do similar, looking for open ports to the internet. It is a poor security practice to have unnecessary open ports to the internet, and this process can identify running services that don't serve a business purpose (a needless attack surface).
- **Train employees** how to identify phishing emails. Many ransomware attacks spread through phishing emails, many of which are engineered to lure victims to click on a link or open a file. Training employees to be vigilant is best practice to avoid a host of other cyber attacks as well.
- **Follow the principle of least privilege**: don't give employees or service accounts entitlements they don't need. In particular, limit "local administrative privileges" to those employees who only truly need it.
- **Practice good password hygiene**. Don't use the same password for multiple administration or service accounts and make sure passwords are complex and reasonably lengthy.
- **Update antivirus** on endpoints and servers and set them to automatically conduct regular scans. This protects the infrastructure if the signature of the attack is known.
- **Properly segment** the network. Identify the most critical assets and data and separate them with network segmentation and strict access control. Each security boundary between segments represents a hurdle for attackers and opportunity for organizations to mitigate an attack.
- Ensure critical systems and files have **up-to-date backups**. This provides the best protection against data loss due to ransomware. Backups should be protected and tested for restore capability.
- Have an **Incident Response Plan and Process** that is up-to-date and tested in place. The severity of many incidents is needlessly increased because of a lack of a timely and appropriate response.

What Can AIG Do For Organizations?

AIG insureds should take advantage of available key complimentary services (if it has not already), including:

- Blacklist IP Blocking
- Employee Security e-Learning Awareness Training
- Infrastructure Vulnerability Scan

We also offer additional fee-based services that would directly support an organization's evaluation of vulnerability to recent attack types, including an Internet Facing Systems Assessment, Cyber Defense Review, and ratings services powered by BitSight and Security Scorecard.

These services have been specifically selected based on our nearly 20 years of experience and how well they can help strengthen the cybersecurity maturity of an organization.

Get started today. Visit www.aig.com/cyberriskconsulting.

06/18