DATA SHEET

Security Awareness Checklist

Beyond compliance. Make an impact. The key to having an effective security awareness program is to start with a simple checklist. This checklist is categorized into three topics: Measure, Mitigate and Educate.

Provided by Symantec Education Services

MEASURE

PEOPLE

Conduct a cost-benefit analysis and identify ways to mitigate risks associated with people, processes and technologies.

PROCESS

Conduct an IT audit via 3rd party. Know your staff, their qualifications. Identify critical assets that reside on the network and the company's network parameters.

Develop an incident response plan. Test it regularly.

Conduct periodic audits of physical access to an organization's locations.

Establish a patch management strategy for all operating systems and applications.

Establish meaningful metrics to gauge effectiveness and impacts of security awareness training.

TECHNOLOGY

Conduct vulnerability scans regularly.

MITIGATE

PEOPLE

Educate staff to lock all devices if they need to leave them unattended for any length of time.

Always close web browser sessions when *not* in use. If at all possible, avoid using the same device for business, banking and personal online activity. Better still, dedicate a device solely for banking.

Be careful when clicking on attachments or links in email. If it's unsolicited or suspicious for any reason, don't click it.

Conduct sensitive browsing activity, such as banking, only on a device and network that belongs to you.

Train staff to be conscientious of what they plug in to devices. Malware can be spread through infected flash drives, external hard drives, and even smartphones.

Share the "Symantec Security Awareness Quick Tips" social media videos, which will extend cyber security acumen beyond the corporate environment and across the lifestyle of each individual.

PROCESS

Establish high-level IT Security Guidelines and supporting directives.

Change culture by implementing an ongoing security awareness training program in varied formats to promote healthy cyber routines.

Establish a comprehensive password program to educate employees on strong, unique password creation. And, don't use the same password for multiple sites.

Monitor accounts on a regular basis for any suspicious activity. If something appears unfamiliar, it could be a sign that account activity has been compromised.

Back up data regularly, and make sure anti-virus software is always up to date.

Use password management software and deploy a group policy to keep network passwords fresh.

Implement badge access to physical workspaces and grant access based on role, privilege or need-to-know.

https://go.symantec.com/awareness

security_awareness@symantec.com

MITIGATE - cont'd

Engage with IT management frequently to discuss current cyber threats. Conduct a cost-benefit analysis and identify ways to mitigate risk.

Establish policy for properly secured remote access.

Obtain cyber insurance and expect the unexpected. Help mitigate the cost of incident recovery, legal fees and crisis public relations (PR).

Implement dual approval and control for indispensable or easy-to-abuse tasks, eliminating a single point of failure.

Implement functionality for Incident Reporting to include infection and incident response procedures.

Implement internal security controls for data. Audit access to where data resides.

TECHNOLOGY

Conduct periodic phishing exercises to test end-users on their ability to identify and report potentially harmful emails.

Implement email technology that filters emails based on domain and email authentication protocol.

Restrict email attachments by configuring email servers to block or remove specific file types.

Implement a secure password storage tool, and deploy server rules requiring password best practices.

Deploy a company-wide VPN to restrict access privileges to confidential company data.

Secure all wireless networks to prevent unauthorized access, eliminating entry points.

Ensure regular backups of critical systems and endpoints are easily available.

Deploy an integrated cyber defense platform to protect data in email, cloud, endpoints, and networks.

Enable 2-factor authentication (2FA) on devices, web applications and for wire transfers.

Deploy a Cloud Access Security Broker (CASB) solution for proper security when using any file sharing or web applications in the cloud.

Deploy an email security solution to monitor both inbound and outbound emails for cyber threats.

Manage Internet access though access control policies and restricting user access to key devices.

Implement a banner message that appears on all incoming email from an external source.

Implement data loss prevention technology and software for visibility, control and protection of sensitive data.

Engage a 3rd party to audit and identify weaknesses with your IT systems.

Implement firewalls and intrusion detection systems.

Restrict USB port access within the organization, based on organizational needs.

Implement protocols for digital signatures on internal emails for verification of authenticity.

Engage with IT management to potentially disable unstable or risky programs such as Flash and Java.

Identify technologies that can help your organization when breached. Know your critical assets.

Isolate threats quickly, preventing infection of individual computers or the network.

EDUCATE

PEOPLE

Realize people are a common target to hackers. Avoid thinking: "It won't happen to me."

Identify top human risks and the behaviors to change through a positive and engaging security awareness training program.

Train staff to be wary offline if someone calls or emails asking for sensitive information. Always call the company directly to verify credentials before giving out any information.

Structure a long-term, ongoing security awareness program that creates a secure culture where people are the first line of defense.

Grow the conversation. Conduct brown bag lunches or virtual sessions that address one security awareness topic at a time.

Be aware of digital footprints. Educate staff about what they should *not* share on social networks, as well as how their own information can be used against them and your organization.

Train staff to verify anything suspicious, especially UNSOLICITED emails from KNOWN or UNKNOWN sources.

Educate employees to only visit work-related websites while at work.

Keep employees educated on the latest threats and remain vigilant against dangers in their Inboxes.

https://go.symantec.com/awareness

security_awareness@symantec.com