5 Hallmarks of an Effective Cybersecurity Program

By John Thackeray

The average cost of a cybersecurity breach is believed to be in the range of $3.7 million, but it's aftereffects can have more far-reaching consequences in terms of operations and reputation.

Every firm is now expected to have a robust cybersecurity program that is based on the five core elements of the NIST Cyber Security Program: identify, protect, detect, respond and recover. The program should be enterprise-wide, capable of being tested, and exhibit clear and transparent metrics. Furthermore, it should outline clear roles and responsibilities, and, to reinforce policy and controls, must communicate established plans (breach notification, security awareness, incident response) for continued development, training and education.

A cybersecurity framework must also be clearly documented. Regulators view non-existing documentation equal to disinterest in the matter. The challenge for any effective cybersecurity program is to implement a comprehensive model that can incorporate the key elements below, which are the 'must haves' for the basic layer of protection.

Now let's take a look, in brief, at the five hallmarks of an effective cybersecurity program:

1. Program Documentation

The program must be clearly documented. In the eyes of regulators, if you do not have documentation, you are not doing anything. Indeed, the program will be worthless unless it is correctly enforced, and regularly checked for suitability.

2. User Security Awareness Program

A well-trained staff can serve as the first line of defense against cyber-attacks. Effective training helps to reduce the likelihood of a successful attack by providing well-intentioned staff with the knowledge to avoid becoming inadvertent attack vectors – for example, by unintentionally downloading malware.

3. Application of Cybersecurity

Here is a list of common cybertechnology controls that can/should be used, depending on resources and materiality:

- Anti-malware technology, such as endpoint antivirus;
- Email scanning (cloud and/or on-premises)/web protection/web proxy services;
- Security information and event management (SIEM);
- Hardening workstations (removing programs such as Adobe Flash);
- Firewall ingress and egress rules and/or next-generation firewall;
- Weekly and monthly patch management (operating and applications systems); and
- Network intrusion system and/or host intrusion.

4. Vulnerability/Incident Reporting /Lessons learned

Planning and preparing for a cybersecurity incident are among the greatest challenges faced by any organization. When a cybersecurity incident occurs, how it is handled will be a reflection on the capability and ability of the management to act and respond. Incident reporting must lead to proactive changes – i.e., employment of new countermeasures, and amendment to procedures; otherwise similar incidents can be repeated with varied success.

5. Key Prevention Techniques

The following common prevention measures are required to prevent in-house breaches:

- Full disk encryption on mobile and portable endpoints;
- Restriction of local administrative and/or domain administrative rights;
- Basic logging of authenticated user activity (logon/logoff events);
- Password management and/or password policies;
- User awareness training /advanced logging of authenticated user activity (folder/file-level auditing)/principle of least privilege (using file share and/or NTFS permissions);
- Snapshot backup/recovery capability; and
- Application white listing – permitting only those applications that have been approved to do so to operate on networks.

Parting Thoughts

Clearly, there is a lot to be absorbed. The abundance of documentation on cybersecurity can lead to fatigue and indifference. The trick, therefore, is to make the cybersecurity program interactive and fun, so that the human firewall can at least mitigate some of the common threats.

John Thackeray is the founder and CEO of Risk Smart Inc. Over his long career, he has held many risk positions, including CRO posts where he interacted and engaged with US and European regulators. He frequently contributes articles on his risk insights to the Financial Executives Networking Group (FENG).