MK Agents

Cybersecurity Report II

TRAINING

Cybersecurity training is a large industry that provides training and information regarding cybersecurity practises and business protection. There are many training courses and certifications that can be provided online or in person, with various training objectives and delivery methods. This is important to the success of a business because, as described in the prior report, security problems can result in large losses, and having awareness of how to handle these issues, from an individual level to a business wide level, can prevent most of these issues from taking place.

Training courses usually have a similar goal in mind with training; they attempt to establish some of the causes of cybersecurity attacks, how to mitigate the chances of these attacks taking place, as well as how to implement analysis and review structures that handle analysing why a previous problem took place in the first place and preventing it from happening again. Consolidating information from multiple sources, some of the key topics are:

- Information about how these attacks take place and how to recognise them, along with specific examples of attack types (i.e. phishing emails and malware)
- Education about the ramifications of cybersecurity attacks, legal, personal and business-wide.
- Risk management techniques.
- Incident Handling methodologies.

(Rayome, 2019) (FraudWatch International, 2018) (Secureworks, 2018)

These topics educate the individuals in the business about some main topics involving cybersecurity awareness and best practises. This kind of training alone is not enough to protect a business from cybersecurity attacks, as there needs to be implementations of administration-level protections, covered later on in this report.

Buy-in is a large issue in cybersecurity, specifically employee and executive buy-in. This is where employees or executives either don't know cybersecurity practises or don't consider cybersecurity practises to be important, either way resulting in them not following best practises and adding to overall risk (SecurityTrails, 2019). There are steps that can be taken to increase buy-in, thereby making the training more effective and having the execution of best practises be more common (Givens, 2019).

POLICIES

Education about cybersecurity risks is a huge benefit to businesses, whether small or large. Human error is impossible to avoid and having only awareness training won't prevent human error from resulting in cybersecurity risks and attacks. According to a study by IBM, human error is the main cause of 95% of cyber security breaches (IBM Corporation, 2014). This indicates that, no matter how much training takes place, human error will always be a risk to cybersecurity.

This can be mitigated by implementing business-wide security policies, much like with physical security, involving specific instructions regarding risk elements leading to potential attacks. Successful policies rely on a few major steps, specifically;

- Policy about handling of risks and what potential risk factors are.
- Reminders of positive habits to help prevent human error.
- Warnings of the ramifications of not complying with the policy.

(BSI Group, u.d.)

The first step involves a procedure for a security risk, usually including how some examples of it, what to look for, and how to deal with problems as they arise. For example, a policy could be put into place about handling found USB devices such as memory sticks, which could damage computer hardware and affect software negatively with malware, for example. This policy would state that any USB devices should be sent to a security or IT team for checking or discarding. As well as this, the policy should include information that *any* USB device could be affected and to not plug anything in, as well as why.

Overall, policies like this rely on informing individuals as well as having structures in place inside the business that deal with security risks. Security teams are often considered for physical security, including CCTV and location security, however cybersecurity should be treated in the same way as it's a similar vector for attacks. A team that handles issues and creates policy based on prior events and discoveries would serve to futureproof the business for any potential upcoming attacks. (Shiver, 2017)

Having this team lead policy and informative training regularly, as well as informative posters, for example, that regularly inform individuals of said policy and education, should they forget or consider it unimportant. This links back to the buy-in section described in the previous section, as having an employees as cybersecurity team members and having regular employees being involved in the process generally results in improved buy-in and therefore cybersecurity safety (Expert Panel, Forbes Technology Council, 2018).

PROTECTIONS

Cybersecurity doesn’t just lie in the realm of the employees and their actions. Training and policy can only get so far in defending against cybersecurity attacks, as the network, software and hardware all have security risks involved that aren’t linked to social engineering and are instead flawed due to software/hardware vulnerabilities and unsafe network design (Rapid7, n.d.) (Bond, 2018).

Depending on the function of a business, there can be important data saved on internal servers including user passwords, user data, business data and more. This information all has special requirements for being stored properly, especially user passwords. Should a network be breached, it’s down to the storage of this data and the network topology to keep the information contained within safe.

User passwords are a great example for data security, as they rely on network security, hardware and software. There are steps that can be taken in network design that protect access to servers that store passwords. A good feature of network security is a firewall, that protects unauthorised access to the server hosting the passwords data. In terms of data security, passwords should be:

- Hashed (one-way encryption) at least once before storing.
- Salted (adding in data to make identical passwords have a different hash output).

(Fredenslund, 2018)

This process effectively makes the stored data useless for anyone who doesn’t have the unencrypted password to begin with. Since it’s a one-way encryption, you can’t get a password back out of the stored/salted hash. This improves data security as, even if the password database were acquired in an attack, it wouldn’t necessarily contain and useable information.

The steps that a business can take in delivering software and network solutions in order to protect against cybersecurity attacks at a low level. Specifications exist for network design, usually focussing on LANs, providing specific information as to how to design and setup a network (Bond, 2018) (Oxenhandler, 2019).

BIBLIOGRAPHY

Bond, R., 2018. *Network Security Design is Critical to Eliminating Security Gaps and Reducing Costs.* [Online]
Available at: https://www.secureops.com/networking/effective-network-security-design/
[Accessed 14th November 2019].

BSI Group, u.d.. *Creating cyber security policies.* [Online]
Available at: https://www.bsigroup.com/en-GB/Cyber-Security/Creating-cyber-security-policies/
[Accessed 14th November 2019].

Expert Panel, Forbes Technology Council, 2018. *Company Cybersecurity: 10 Ways To Build Employee Buy-in.* [Online]
Available at: https://www.forbes.com/sites/forbestechcouncil/2018/11/29/company-cybersecurity-10-ways-to-build-employee-buy-in/#42494ecc70d9
[Accessed 14th November 2019].

FraudWatch International, 2018. *What is Cyber Security Awareness Training and Why is it so Important?.* [Online]
Available at: https://fraudwatchinternational.com/security-awareness/what-is-cyber-security-awareness-training/
[Accessed 14th November 2019].

Fredenslund, K., 2018. *How To Securely Store User Passwords.* [Online]
Available at: https://kasperfred.com/posts/how-to-store-user-passwords-securely
[Accessed 14th November 2019].

Givens, S., 2019. *Five Strategies To Get Employee Buy-In For Security Awareness Training.* [Online]
Available at: https://www.forbes.com/sites/forbeshumanresourcescouncil/2019/04/12/five-strategies-to-get-employee-buy-in-for-security-awareness-training/#6f65068f236d
[Accessed 14th November 2019].

IBM Corporation, 2014. *IBM Security Services 2014 Cyber Security Intelligence Index,* New York: SCMagazine.

Oxenhandler, D., 2019. *Designing a Secure Local AreaNetwork.* [Online]
Available at: https://www.sans.org/reading-room/whitepapers/bestprac/designing-secure-local-area-network-853
[Accessed 14th November 2019].

Rapid7, n.d.. *Vulnerabilities, Exploits, and Threats.* [Online]
Available at: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/
[Accessed 14th November 2019].

Rayome, A. D., 2019. *3 things you need in a cybersecurity awareness training plan.* [Online]
Available at: https://www.techrepublic.com/article/3-things-you-need-in-a-cybersecurity-awareness-training-plan/
[Accessed 14th November 2019].

Secureworks, 2018. *Cybersecurity Awareness Training: Threats and Best Practices.* [Online]
Available at: https://www.secureworks.com/blog/cybersecurity-awareness-training-best-practices
[Accessed 14th November 2019].

SecurityTrails, 2019. *Cyber Security Culture: Why It Matters for Your Business.* [Online]
Available at: https://securitytrails.com/blog/cybersecurity-culture
[Accessed 14th November 2019].

Shiver, B., 2017. *How to build a cybersecurity team.* [Online]
Available at: https://www.cio.com/article/3219371/how-to-build-a-cybersecurity-team.html
[Accessed 11th November 2019].