itworldcanada.com

Understanding cybersecurity management for FinTech: cybersecurity policy and strategy management (Article 6) - IT World Canada

Gurdip Kaur and Arash Habibi Lashkari

8-10 minutes

Cyber-attacks are on the rise with every passing day, and so is the cost associated with the damage caused by them. To protect the financial institutions from the menace of these cyber-attacks, a cybersecurity policy and strategy sets the standards to: monitor cyber activities on premises, design prevention and detection measures, and take appropriate actions to curb these activities.

Cybersecurity follows a “layered security” approach, which provides “Defense in Depth”. This is the practice of combining multiple security controls to monitor, detect, and thwart cyber-attacks. Relying on a single security control for providing a complete security solution is never recommended by cyber professionals, as every security control has its limitations and boundaries. Cybersecurity policy and strategy are designed to tackle growing cyber-attacks on financial institutions, responding to the menacing consequences of sophisticated cyber threats.

This article provides a comprehensive introduction to various cybersecurity policies and strategies used to protect FinTech institutions from belligerent cyber-attacks. The content in this article is based on the extensive research work behind our book titled *“Understanding Cybersecurity Management for FinTech”* published by Springer this year.

Cybersecurity policies and strategies

The fundamental requirements to prepare a cybersecurity policy and strategy are to know details including: assets, people, business objectives, potential threats, disaster recovery plan, business continuity plan, and security awareness program. Cybersecurity policy needs to be aligned with business objectives so that business continuity is not disturbed, even during a security incident. Figure 1 presents an overview of cybersecurity policies.

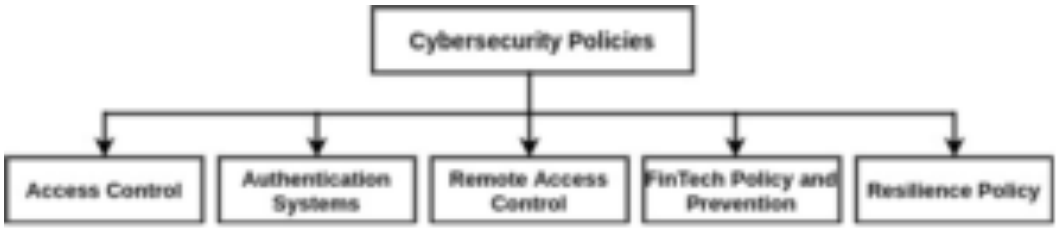

Figure 1: Cybersecurity policies

Access control

Controlling access to the assets is one of the main controls provided by the central theme of security. Access control prevents unauthorized personnel from accessing a piece of information. It not only controls unauthorized access, but also provides a relationship between different entities; granting and restricting access based on a user’s identity. Access controls can be

classified into three categories: preventive, detective, and corrective.

- **Preventive access controls** attempt to stop or prevent unauthorized activity. For example, using fences and locks to secure a physical location.
- **Detective access controls** are sometimes classified as preventive controls. Detective access controls attempt to detect or identify unwanted or unauthorized activity. These controls come into action after the activity has occurred. Some examples include CCTV or security cameras.
- **Corrective access controls** modify the environment to return systems to their normal status after a policy violation. Recovery access controls are classified as corrective controls.

Authentication systems

Authentication is the process of testing or validating the claimed identity of a user. It requires the user to provide additional information to prove his identity. The most common form of authentication used is passwords. Following are the common types of authentication methods used nowadays.

- **Password-based authentication:** Passwords are the most common method of authentication. A strong password is a combination of lowercase and uppercase characters, numbers, and special symbols. Passwords can be stolen easily.
- **Multi-factor authentication:** It requires more than one method to authenticate the user, for example, a combination of password and CAPTCHA. It adds a layer of security to access the user account.

Sometimes, challenge questions are answered by the user before logging into the account. The answers to these questions are provided by the user and stored in the system at the time of registration.

- **Biometric authentication:** Biological features such as retina, fingerprints, and voice and face recognition are unique for every individual. They cannot be stolen or hacked. Thus, they are more secure than password-based authentication and multi-factor authentication.
- **Certificate-based authentication:** Digital certificates can be used to identify a user, system, or device. A digital certificate is an electronic certificate that contains the digital identity of the user. It contains a public key issued by the certification authority. The corresponding private key of the public-private key pair is kept safely with the user. A combination of the public and private key is used to prove the identity of the user.
- **Token-based authentication:** It uses an encrypted string of random characters called a token to authenticate users. The credentials are entered only once, and the token is used over again by the user.

Remote access control

Remote access policy defines the standards for connecting to a computer from any host computer outside the organization. The policy is designed to minimize the potential exposure to FinTech institution from damage resulting from the unauthorized use of their resources.

FinTech policy and prevention

The cybersecurity policy addresses cybersecurity principles for regulators, policymakers, supervisory committees, and service providers. These policies promote cyber hygiene, educate users, and limit cybersecurity incidents. Some effective cybersecurity policies to prevent cyber-attacks in FinTech are briefed below.

- **Establishing and using firewall:** A firewall is a system designed to protect against unauthorized access to or from a private network. Firewalls manage, control, and filter network traffic.
- **Installing and using antivirus:** Antivirus software scans all applications, files, and devices to identify any known malicious activity. It offers little or no protection against unknown or zero-day malware.
- **Removing unnecessary software:** Unnecessary software may be installed intentionally by the user, or may get installed along with legitimate software. Unnecessary software includes applications and software that the user does not use anymore. Whatever the case be, it is essential to uninstall unnecessary software from the computer or mobile phone due to several important reasons, including memory space taken by them and malicious activities that illegitimate software can perform.
- **Applying updates and patches:** Updates and patches fix a known or identified vulnerability in software, application, or operating system. The vendors regularly release them.

Resilience policy

Cyber-resilience policy provides the capacity to withstand, recover

from, and adapt to external shocks caused by cyber risks. It prepares organizations to face adverse events and continue business in those conditions. The basic principles of a cyber-resilience policy include simple regulations, internationally harmonized, principles-based, and risk-based. It maximizes resilience while minimizing risks. The main characteristics of a cyber-resilience policy for FinTech institutions are:

- **Cyber-hygiene:** Cyber-hygiene is the basic characteristic of a cyber-resilience policy. It ensures that users are cyber educated. There are always software flaws and unpatched vulnerabilities that pose severe damage to the institution after attackers exercise them. The main concern of a cyber-resilience policy is to get rid of these flaws and unhandled vulnerabilities. Regular updates and installation of patches are the basic steps needed to cover these flaws.
- **Timing of cyber incidents:** Advanced persistent threats may remain hidden for a long time without getting noticed. This means that institutions may succumb to a false sense of security that makes them more vulnerable.
- **Operational and business impact:** Cyber-attacks impact information systems and have a high impact on operations and business. The most severe cyber-attacks may cause systemic risk, letting the entire infrastructure down. This raises concern over business objectives that must consider cyber-resilience policy while designing, planning, and implementing business strategies and policies.

Conclusion

By following fundamental cyber practices and educating users, employees, and people within the organization on various cybersecurity policies and strategies, threatening cyber-attacks within FinTech institutions can be prevented.