CYBERSECURITY STANDARDS FOR COMPANIES
Basic protocols required for secure digital transactions

Maryland-based businesses today must recognize that state and federal agencies are now regulating businesses in the area of cybersecurity, and that shareholders and customers expect them to have strong cybersecurity measures in place. The below outlines the practices and protocols for secure digital transactions.

What standard of care is expected when doing business in cyberspace?

The standard of care is due diligence. A reasonable process must be in place. All employees of the company must adhere to reasonable cybersecurity measures and must know what steps to take based upon variables. The level of a company's security practices must be commensurate with the sensitivity and volume of consumer data to which it has access as well as the complexity of the business operation.

Example: A company must ensure that its staff is able to and does implement "patches" when updates become available to address a known vulnerability in order to protect consumer data.

What are the three principles of cybersecurity that guide the creation and implementation of a company's program?

Confidentiality, Integrity, and Availability

Example: A trifecta approach to security is protecting individual data sources and/or data on a network (confidentiality), ensuring this data does not get altered or corrupted (integrity), and ensuring that the data can be accessed and retrieved when needed (availability).

What is the freezing an account requirement?

This is a mandate to suspend or disable a user's account after multiple unsuccessful login attempts.

Example: Businesses are to implement automatic freezing of account in certain situations. To fail to freeze an account in such situations would put businesses networks at risk, and in turn would place customers' information at risk for exploitation.

What is the prohibition on storing user credentials in plain text?

User credentials cannot be stored in clear, readable text.

Example: The Federal Trade Commission can charge companies for failure to store credentials properly, especially for failure to securely store credit card information. To implement proper protection, businesses must have a practice so administrative passwords are not sent in plain text in personal email accounts.

What does storing credentials securely mean?

Customers' personal data, financial transaction data, and administrative passwords must be encrypted at rest, and must be subject to additional measures, such as two-factor authentication.

Example: To allow one's access to data, two-factor authentication requires two methods to verify one's identity. One method is 'something you have' (i.e. a certificate); another could be 'something you know' (i.e. a password); and a third could be 'something you are' (i.e. a biometric characteristic). Most of us are familiar with two-factor authentication (a card with a chip and entering a PIN). Two-factor authentication means two elements must be met to restore or obtain an updated password (such as providing a specific personal question *and* something specific about the account) for successful verification of credentials.

What is the requirement to protect against authentication bypass?

Hackers use known common vulnerabilities and run scripts against a website. Thus, companies must test their web applications for widely-known security flaws to ensure their networks are protected against authentication bypass. The requirement is for companies to use proper cybersecurity due diligence in their digital networks.

Example: Without technical protocols in place, a hacker could predict patterns and bypass the web application's authentication screen and gain authorized access. Widely-known security flaws are often published and companies have an obligation to "patch" the vulnerabilities. In some cases, businesses do not exercise prudent reviews and fail to patch. Hackers know this, and exploit them, by trying multiple websites with a similar hacking method to exploit the widely-known security flaws.

Why are US companies adopting secure remote access more frequently?

With the rise of telecommuting, mobility, and the demand to access work files ubiquitously, companies are implementing more secure remote accesses for their employees. Secure remote access also leaves confidential, personal privileged and/or proprietary data on a company's home network (versus an employee's home laptop or mobile device). This approach is one demonstration of a company's due diligence and a commitment to cybersecurity best practices.

Example: Secure remote access today is generally through use of a VPN, SSH, or SSL tunnel.

What are three areas in which businesses need to invest to limit unauthorized access to proprietary and personal data by both outsiders (non-employees) and insiders (employees)?

Administrative, Technical, and Physical Access Controls. Administrative controls are internal company processes or training, which are understood and implemented by all employees.

Technical controls are protocols that automatically occur through software, hardware or firmware triggering mechanisms. Physical access controls are items that permit physical access to data only when necessary for performance of duties.

Examples: Administrative controls include keeping current standard operating procedures in place and training employees whenever updates occur (but no less than once a year). Technical controls include automatic freezing of account after unsuccessful multiple logins attempts, as well as encryption and firewalls. Physical access controls include both people (security guards) and objects (uniquely locked doors to data center or hard drives). These three consistent business practices, used together, demonstrate due diligence and layered defense in a cybersecurity program.

Ms. Janosek, Esq., is a member of the federal Senior Executive Service in Maryland and is a Certified Information Systems Security Professional, and focuses on cybersecurity.