Don't Plan to Fail: Putting Data Security into Practice

Data security is one of the most important aspects of any business, and for the credit professional, perhaps more so. Securing payment details and other confidential information is vital in an age of hackers and cyberattacks.

In the world of data security, if you fail to plan, you plan to fail, according to *Cyber Risk: Practical Actions to Improve Data Security*, from law firm Allen & Overy. Cyber breaches can be prevented with the right procedures and policies in place. Policies should be documented in regards to data security and encryption of data. Scan removable media, such as thumb drives, for malware before connecting them to your systems. Keep all IT systems current by applying updates and patches in a timely manner. Also consider how your data is stored and whether the backup systems are secure as well.

Securing data should be a multistep process, said Anton Goddard, president of NACM South Atlantic. Firewalls and establishing secure passwords are just some of the steps of data security. No personal information should be stored unless it is encrypted. “Any information that gets out would be a loss of trust,” he said. “Whether it’s confidential or not, no one wants to see that their information is out on the internet.” Most of the risk comes from customers storing credit card numbers on their computers or emailing the information, he added. The credit card information in an email is stored on backup servers, which leads to vulnerability.

Training of personnel is also an important consideration. All those involved in your data systems should be kept aware of the processes you have in place to prevent cyber breaches. This includes a clear allocation of risks and governance responsibilities, from minimum requirements to incident management, according to Allen & Overy. Cyber response insurance can help in the immediate aftermath of an incident by identifying weaknesses and restoring data security. In lieu of insurance, be sure to have contact details of a company or expert that can assist in case of a breach.

Personnel should know how to identify trusted communications. Cyberattacks are often carried out by mimicking genuine communications such as email. A pro-reporting culture should be encouraged to help you to quickly discover any attempts to infiltrate data systems, Allen & Overy says.

Often it is not the data control environment itself that is the weak link in the chain, but rather the action or inaction of personnel that leads to security incidents, according to the Payment Card Industry's (PCI) Security Standards Council. Disclosure of information in a social engineering attack, not reporting unusual activity and accessing information unrelated to the user's role without following proper procedures are some of the vulnerabilities outlined by the PCI.

Organizations need to have a security awareness program in place so that employees know the importance of protecting sensitive information. A successful awareness program may include assembling a security awareness team and establishing a checklist when developing, monitoring and maintaining a security awareness training program. The PCI recommends that the security awareness team be staffed with employees from different areas of the company who have a variety of responsibilities to represent a cross section of the organization. Security awareness should be conducted on an ongoing basis. The depth of awareness training should increase with the level of risk connected to different roles within the company.

With these and other steps put into practice, credit professionals can more fully rest assured that their data is protected.

– Adam Fusco, associate editor