Network security

How to deter and mitigate the fallout from cyber attacks

KRISTEN WERRIES COLLIER
Partner
Novack and Macey LLP

(312) 419-6900
kwc@novackmacey.com

WEBSITE: Visit www.novackmacey.com to learn more about this and other legal issues.

Insights Legal Affairs is brought to you by **Novack and Macey LLP**

Is the confidential information on your network safe? That's a question every organization should ask itself because network security breaches are common and becoming even more prevalent.

Kristen Werries Collier, a partner with Novack and Macey LLP, says organizations must acknowledge this risk and vigilantly monitor and evaluate their cyber-security safeguards and protocols to minimize it.

Smart Business spoke with Collier about network security breaches and the steps companies can take to mitigate or eliminate them.

How common are enterprise security breaches?

Most large and mid-size companies have confronted a cyber attack at some point. Network security attacks are a reality you must confront head-on. The threats to your network posed by unauthorized access — and the damage caused by a successful attack — will only continue to rise.

Can you prevent a security breach of your network?

While you may not be able to prevent a breach with absolute certainty, you can certainly deter one by proactively assessing and addressing your network's vulnerabilities. If you don't have the in-house expertise to do that, consult a security adviser. You want to invest your money in safeguards that deter — if not prevent — the attacks you are likely to face and a security adviser can identify those for you.

Keep in mind that no system is ironclad because hackers adapt as security measures evolve. Accordingly, you must routinely monitor your layered security measures to make sure you are keeping up with determined hackers. Avoid being the easy target.

What should you do if, despite your precautions, a breach happens?

Undertake these best practices:

- Act fast. Perform a post-attack forensic analysis to determine the 'who, what, when, where and how' of the breach. You'll need to preserve this information to evaluate the damage, mitigate the fallout, structure appropriate remedial measures and build a case against the hacker.
- Promptly notify anyone whose sensitive information may have been compromised.
- Update your intrusion detection and prevention systems and other safeguards to deter future breaches.
- Assess what your legal obligations are in the wake of the infiltration.

What is the potential fallout if your network is breached?

Breaches expose your organization to legal claims and undermine its competitive advantage. As for the legal claims, the law mandates the protection of certain types of information like consumers' personal and nonpublic financial information, social security numbers and medical records. Your organization could potentially face claims predicated on an array of legal theories, including: negligence; breach of contract; the Fair Credit Reporting Act, which subjects certain organizations to liability if they fail to safeguard consumer credit information in their possession; and Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices affecting commerce.

While you may defeat such legal claims on a motion to dismiss or ultimately at trial, it will cost you money to do so. From a business perspective, a security breach may have financial and competitive repercussions by publicly exposing your organization's highly confidential or propriety information and by eroding consumer confidence in doing business with you.

What, if anything, is the government doing to crack down on hackers?

The government is cracking down by charging hackers with crimes carrying potential years of imprisonment and hefty monetary fines. However, the deterrence effect of this crackdown is somewhat limited given that numerous hackers operate outside of the U. S., making prosecution difficult, if not impossible. This is yet another reason to deter, if not prevent, a breach of your organization's network in the first place and quickly mitigate the fallout if one occurs despite your best practices. ●