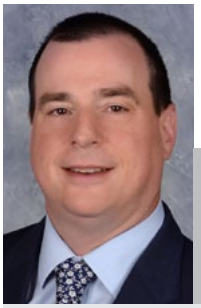
Break it yourself

Mitigate cyberthreats by testing your network for vulnerabilities

INTERVIEWED BY ADAM BURROUGHS



JOE COMPTON, CISSP, CISA, QSA, CICP
Principal, Skoda Minotti
(440) 449-6800 ext. 7252
jcompton@skodaminotti.com

Website:
Are your network and web applications secure? Find out at skodaminotti.com/offer.

Cybersecurity has become a necessity for every business, regardless of size or industry. A hack that results in loss of client information could result in fines or jail time if it was a protected class of information — as is the case with medical records — and the company did little to protect it. Even if unprotected information was lost, a breach of any customer data could mean irreparable damage to a company's reputation.

"In many cases, basic controls such as firewalls do a reasonably good job of keeping the bad guys out," says Joe Compton, CISSP, CISA, QSA, CICP, a principal at Skoda Minotti. "What many companies don't protect is the data leaving its network perimeter. Viruses can get past sophisticated protective software through social engineering attacks that are delivered via email from a recognized sender. Clicking an innocuous link from a seemingly trusted source could cause a major breach. That's why it's necessary to understand the unique risks that face your company and implement controls designed to protect it where it's most vulnerable."

Smart Business spoke with Compton about finding and eliminating weak points in company systems that could otherwise leave companies exposed to cyberattacks.

What liabilities might a breached company face as a result of its inability to keep data secure?

A company's liability varies based primarily on the type information lost and the steps the company had taken to prevent a breach. There are significant monetary fines and possible jail time for a breach of health care information if a company failed to take reasonable steps to protect that data. In banking, regulators could close a bank if IT controls were deemed missing or inadequate to protect nonpublic customer information.

> "While companies can't ensure a breach will never happen, they must do all they can to protect their sensitive information"

Businesses that handle unregulated information and are breached risk a damaged reputation. They can survive such a breach, but rebuilding consumer confidence can be complicated and expensive.

What is a compliance framework in the context of cybersecurity and when is it necessary or prudent for a company to establish one?

A control framework provides an outline of safeguards to consider implementing in specific areas to mitigate risk and secure information that's vulnerable to a company. Some are industry specific, such as Payment Card Industry Data Security Standards for merchants, Health Information Trust Alliance CSF for health care entities, and the International Standards ISO/IEC 27001 framework for information technology.

Industry and type of information stored aside, companies should take these basic steps to learn more about their risks:

- Understand what information they posses and classify it — who internally can see what information, what should be restricted and why.
- Figure out where that information lives — on workstations, in the cloud, and or, on a server or servers in the office.
- Determine what information is critical to day-to-day operations.

These are the first steps in deciding what controls are best suited to protect company information.

How can companies know that the cybersecurity measures they've implemented are adequate?

It starts with a risk assessment. This inventories items such as hardware, software and data, and explores the risks and threats around those based on day-to-day business operations.

A vulnerability assessment is used to test those inventory items for weaknesses so that the control structure around them can be improved. Once the control structure is implemented or enhanced, a penetration test is conducted to see if a security engineer can break through the new controls.

Security is maintained through a cycle of risk assessment and updating the control framework to address the risks identified. It's a process companies will want to repeat at least annually.

There's no such thing as perfection when it comes to cybersecurity, but there are steps companies can take to significantly reduce the risk of having their systems compromised. Control frameworks show a company took reasonable steps to protect customer information and reduce threats. While companies can't ensure a breach will never happen, they must do all they can to protect their sensitive information. ●

With each Insights, Skoda Minotti explores the most pressing problems that manufacturers, and other businesses, face throughout their life cycle.

Insights Accounting & Consulting is brought to you by **Skoda Minotti**