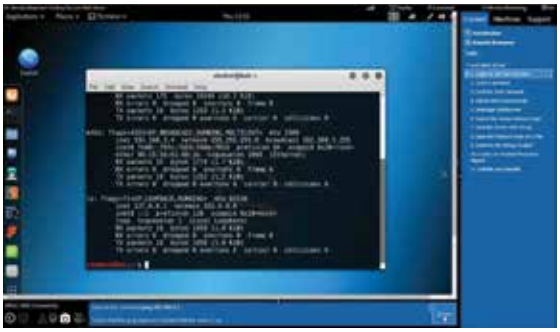
CSX™
CYBERSECURITY NEXUS

MANAGING RANSOMWARE:
Now It Is a Board Issue

Major damage caused by global "NotPetya" attacks in June 2017 quickly elevated ransomware from an IT perimeter security issue to a pressing board of directors-level concern.

This Petya variant revealed a new, more dangerous extortion ware — one that doesn't just freeze or steal data and intellectual property, but destroys data and disrupts systems and company operations. Boards around the world — especially in healthcare, finance, retail, government and infrastructure — took more serious notice of new risks to organizational finances, liability, reputation, worker and customer safety, and future growth.



Destructive attacks like ransomware require updated business continuity plans that minimize downtime and dangers to employees and customers.

A new ISACA report, *Cybercrime: Defending Your Enterprise: How to Protect Your Organization from Emerging Cyberthreats*, identifies ransomware (along with attacks on IoT and cloud services) as a top-three threat for 2017. More than 80 percent of respondents in another ISACA poll expected more prevalent ransomware attacks in the second half of 2017.

6 Strategies for Defeating Ransomware in Your Enterprise

What actions can boards and security leaders take to prevent their companies from becoming victims of brand-damaging ransomware and other cyber extortion? New research and guidance from ISACA and industry experts recommend current and emerging strategies for managing this fast-growing risk. They include:

> "Ransomware has rapidly become one of the biggest cyber security threats in the world."

Understand the threat. Ransomware has rapidly become one of the biggest cyber security threats in the world. As of May, **100,000 organizations in 150 countries have been affected;** ransomware instances in exploit kits have increased about 44 percent in 2017. ISACA's *State of Cyber Security 2017* survey found 62 percent of enterprises reported ransomware attacks, and of these 14 percent were attacked daily or weekly. In the U.S., the FBI estimates that more than 4,000 cases of ransomware occur daily, quadruple the 2016 rate, costing organizations roughly $1 billion per year.

Recognize board and CISO roles. Ransomware's disruptive and destructive new powers clearly fall under directors' responsibility to provide informed oversight and guidance to manage risk, protect assets, ensure compliance with applicable laws and regulations, and represent shareholder interests. The proposed *Cybersecurity Disclosure Act of 2017* would mandate closer partnerships between security leaders and public company boards. Companies that do business in Europe are becoming familiar with the EU General Data Protection Regulation for multinationals, which becomes effective in May, 2018. The growing ranks of chief information security officers (CISOs), up 15 percent in 2017, have a key role to play in informing and advising boards on this emergent threat. ISACA Vice Chair Robert A. Clyde notes that using COBIT provides ones of the best frameworks for clearly reporting cyber risk to top management and boards.

CSX CYBERSECURITY NEXUS

MANAGING RANSOMWARE: Now It Is a Board Issue

Master the fundamentals. Good news: Many security professionals and boards are already engaged in foundational cyber security awareness and activities that can provide powerful protections against ransomware. These include: mapping, regularly backing up and evaluating risk to enterprise data, especially “crown jewels”; restricting network access according to the principle of least privilege; and ensuring the use of robust firewalls, intrusion detection systems, endpoint protection and anti-virus technology. Clyde, in a blog post for the National Association of Corporate Directors, endorsed "Trusted App Listing" (whitelisting) as an excellent control against ransomware and similar attacks.

Conduct awareness training. Half of respondents polled by ISACA immediately after the Petya attack said their organizations were providing staff with ransomware awareness and prevention training, often in recurring quarterly blocks. Nearly one-third of companies surveyed invest $1,000- $2500 per person for training security professionals, ISACA’s *State of Cyber Security* 2017 report found. Overall, more than 35 percent of respondent organizations plan to increase security training allocations.

> **“The Petya variant revealed a new, more dangerous extortion ware… (that) destroys data and disrupts systems and company operations.”**

Update contingency and continuity plans. Compared to the theft of intellectual property or customer data, destructive attacks like ransomware require updated business continuity plans that minimize downtime and dangers to employees and customers. Enterprises should actively develop and regularly exercise plans and response procedures in advance of ransomware incidents. Such planning can include conducting “tabletop” exercises or discussing payment or non-payment decisions. Deliberating these in advance — even implementing a governing corporate policy or other operating guidelines — can help ensure the best decisions, including those at the board level, are made during the heat of a ransomware attack.

Review cyber insurance. Organizations should determine whether their cyber insurance covers ransomware and other new risks, advises *The Harvard Law School Cyber Security Trends for Boards of Directors.* Traditional policies have focused on privacy breaches, the publication notes, but companies should consider re-adjusting policies to include coverage for cyber extortion, digital asset restoration, and business interruption coverage, including systems failure.

Ransomware represents a large, fast-growing variety of overall global cybercrime, forecast by Juniper Research at $2.1 trillion by 2019. More than two-thirds of enterprises surveyed by ISACA believe their boards have adequately prioritized security for ransomware attacks. But only 55 percent agree their board is doing all it can to safeguard digital assets and records. Clearly, building a truly robust posture and defense against ransomware means many enterprises and boards still have work to do.

For more information and resources for your enterprise, go to https://cybersecurity.isaca.org/info/cyber-aware/index.html

Sources:
Cybercrime: Defending Your Enterprise: How to Protect Your Organization from Emerging Cyberthreats, ISACA white paper
State of Cyber Security 2017, ISACA white paper
"Better Tech Governance Is Better for Business," ISACA survey