Managing Cyber Risk As A Business Issue

Ransomware and Cyber Attacks—insider, outsider and even nation-sponsored—threaten your organization's very ability to operate. You could lose millions of dollars in a single Cyber Attack. How will you guard against the threat?

Cyber Attack events

Two major shipping companies suffer weeks of operational delays and disruptions, with $264m USD and $300m USD in total costs and lost revenue—all due to the NotPetya malware.

Global pharmaceutical company experiences total disruption to its drug production business when ransomware takes key production control systems and worker endpoint devices hostage.

Consumer confectionary giant's production stops after NotPetya infects several factory computer systems, inflicting costs of about $140m USD.

Two shifts have moved Cyber Security from an IT issue to a critical business issue requiring Board and C-Level attention:

1. The threat of a Cyber Attack is no longer "if" but "when." Traditional perimeter and detection defenses alone are no longer sufficient to protect your organization: "If a sophisticated attacker targets a company's systems, they will almost certainly breach them."1
2. Increasingly, the outcome of a successful breach has shifted from data theft to data ransom and destruction. These attacks can slow or stop operations for days, weeks or longer – perhaps even permanently – and threaten the very viability of your organization.

Why you care?

There are two key reasons. First, regardless of industry, regulators now focus on Cyber Security. Today, regulators in financial services, healthcare and utilities / energy are drafting new regulations and increasing their emphasis on cybersecurity during audits and investigations. Stronger control paradigms will become requirements soon. As a relevant example, the New York State Department of Financial Services Cybersecurity Regulation requires a written cybersecurity policy to be implemented and maintained, and the Board or a senior officer must annually certify compliance.

Second, the potential damage from a successful cyber attack is so significant that the Board must be involved with cybersecurity to fulfill its fiduciary responsibilities. In an extreme case, a successful attack could delete or encrypt the data and systems that the organization must access to operate. Across industries, key systems may include finance and accounting – especially for publicly traded companies with quarterly reporting requirements and Sarbanes-Oxley oversight. There's no room for these systems to be unavailable or lost. Additionally, specific industries depend on systems crucial to ongoing operations:

Retail	Order management, inventory, and fulfillment
Professional Services (Legal, Consulting)	Document management, time, and billing
Government / Public Sector	Tax rolls, licensing information, and dockets
Healthcare	Electronic medical records, clinical systems
Utilities	Smart meter data, interfaces to industrial systems
Financial Services	Customer accounts and positions, trading systems, and treasury

Imagine the damage to your organization if these systems and their related data (and backups) were permanently and irrevocably lost to a Cyber Attack. And while the damage from an attack directly harms the organization, the subsequent fallout might include SEC reporting obligations for publicly traded companies incurring material losses, and class-action or other significant litigation from shareholders that might include allegations potentially triggering personal liability for Board members.

What should you do?

The Board and C-Level need to take an active, informed and interested role in cybersecurity and managing related risk. They must:

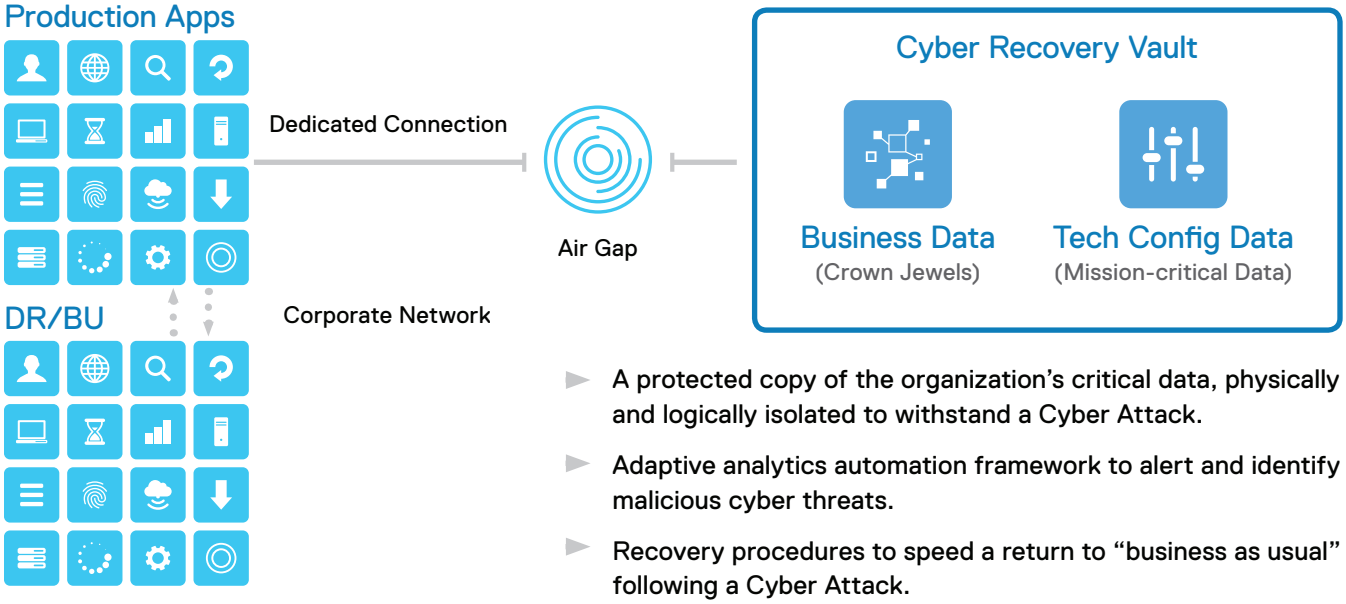
- Provide oversight and direction to create and update policies, procedures and operations related to the organization's cybersecurity posture.
- Assure regular reporting on Cybersecurity status and alerting to the Board, C-Level and other key members of the organization. Regular updates and Board discussion are not only best practice, but can also help to insulate the Board from personal liability if the worst does occur.
- Understand the gaps between risk tolerance and the organization's cybersecurity posture. They then determine whether these gaps are acceptable, need to be closed, or should be covered by cyber insurance.
- Review the organization's ability to recover from a successful cyber attack. This process may have some similarities to disaster recovery / business continuity, but the differences are important. How can the organization recover if production data and backups were deleted or encrypted?

Creating a comprehensive approach to cyber-risk mitigation requires organizations to evolve their recovery and business continuity strategies in addition to focusing on threat detection and remediation. The Dell EMC Cyber Recovery Solution provides organizations with easy to deploy end-to-end Automation and Management Software for realizing workflows to help meet those requirements.

1 - Cyber-Risk Oversight, Director's Handbook Series, NACD.

"Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect that the cyber attack will impact results negatively by USD 200-300m."
—CEO of a major shipping and logistics company

The Solution: A Risk-based Replication Process



- A protected copy of the organization's critical data, physically and logically isolated to withstand a Cyber Attack.
- Adaptive analytics automation framework to alert and identify malicious cyber threats.
- Recovery procedures to speed a return to "business as usual" following a Cyber Attack.

More information on Dell EMC Cyber Recovery Solutions: https://www.dellemc.com/cyberrecovery

Follow Dell EMC Data Protection:

DELL EMC