Cybersecurity Risks and Rewards
How Much Should CEOs Worry About Cybersecurity?
What Should CEOs Do to Minimize Risk?

A Working Paper of the EastWest Institute Breakthrough Group
Strengthening Critical Infrastructure Resilience and Preparedness

Information and communications technology and connecting to the Internet are indispensable tools for business today. They provide essential economic and operational benefits. But they also create risks that must be managed.

Operating a business means taking risk. Without risk, there is no return to shareholders. Businesses face a variety of risks every day, including natural disasters, unfavorable changes in law or regulation, currency fluctuation, unreliable suppliers, untrustworthy employees and, of course, competition. But taking risks that do not create at least equal benefits—a positive, risk-adjusted return—is just bad business.

Most CEOs understand instinctively, based on experience, how to identify and evaluate most kinds of risks. They know their "risk appetite" and understand that risks may interact with each other. Based on their understanding of the enterprise's risk portfolio, and their sense of the likelihood and impact of any particular risk, CEOs decide what risks to accept, to reduce or transfer to others, and to avoid.

That intuitive understanding may fail, however, when trying to assess a complex technological risk such as cybersecurity risk. For any business today, the likelihood and impact of cyber risks are rapidly increasing. CEOs may well be surprised when a cyber breach occurs, and has a significant impact on the business.

The massive data breach at Target ended the 35-year career of CEO Gregg Steinhafel. His resignation is a stark reminder of the predicament faced by CEOs caught in cybersecurity crises. Cyber attacks are continually becoming more sophisticated, making it difficult for enterprises to stay ahead of the adversary.

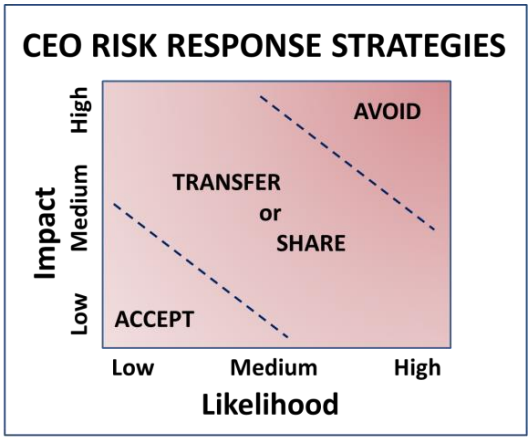
Cyber risks can affect business operations by degrading one of the three elements of information or information technology that are critical to the business—confidentiality, integrity and availability.

The ***Cybersecurity C-I-A*** is at the center of cyber risk management.

Damage to the confidentiality, integrity, or availability (the C-I-A) of business information can cause:

- Loss of revenues,
- Reduced profits,
- Damage to reputation,
- Degraded service levels,
- Legal liability.

Different impacts and damage are caused by different attack techniques (see box). Some attackers will use more complex techniques, such as stealing confidential information and threatening to reveal it (extortion).



News reports tend to focus on the more spectacular kinds of attacks—those seeming to come from foreign governments, terrorists or criminals. But most damage comes from competitors, or from service professionals or suppliers who have poor cybersecurity. These trusted business partners can put a company at risk inadvertently.

Types of Attack and Damage	C	I	A
Denial of Service			✓
Theft of Information	✓	✓	✓
Destruction of Information		✓	✓
Modification of Information		✓	
Hijacking of Technology		✓	✓

Inside Threats	Outside Threats
Dishonest or unhappy employees	Competitors
Careless or unaware employees	Service professionals (attorneys, accountants)
Outdated technology	Suppliers, vendors
Weak security implementation	Criminals, terrorists, governments

In addition, many businesses focus primarily on outside threats, when in truth there are as many risks arising from poor practices or malicious individuals inside the company.

Cybersecurity engineers and managers know that it is impossible to avoid all these risks. Defensive technologies and techniques can almost always be defeated by a determined and persistent attacker. Some careless employee will inevitably open an infected file that looks like it came from someone they know. At that point, the enterprise network and the information on it are on the way to compromise.

Step One: The Five Cybersecurity Risk Questions

The CEO should start by finding out how well his risk management team understands the cybersecurity risk landscape. One way to get there is to ask five key cybersecurity risk questions. These questions are not much different than the questions one might ask about other common business risks, and that is the point. As these questions confirm, managing cybersecurity risk is like managing other risks. It requires a common sense approach and reliance on technical expertise that the CEO may not have.

Experience teaches that most companies are unable to provide convincing answers to questions 3, 4, or 5. The cybersecurity risk landscape is very complex, and new risks arise regularly. Residual risk is thus somewhat open-ended. But known residual risks are identifiable. Similarly, prioritization of investments in cybersecurity is difficult because of the relative immaturity of the field. There is little data to support a quantitative tradeoff between, for example, training employees about

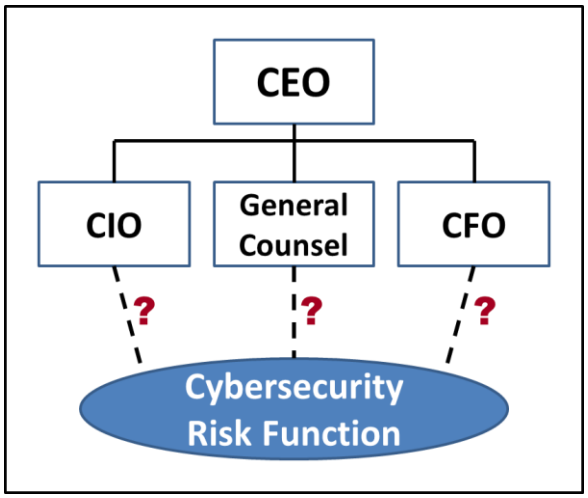
1. What key information and technology assets are we trying to protect?
2. What are the major cybersecurity risks that could affect our business operations and profitability?
3. What techniques are we using to mitigate those risks?
4. What residual risks remain after we have applied those techniques?
5. How did we decide where to prioritize our risk management expenditures and efforts?

malicious attachments versus purchasing a better firewall.

The most important thing to remember is that the answer to question 1, “What are we trying to protect?” defines the answers to all the other questions!

Step Two: Create the Right Lines of Responsibility

If you asked these five questions to your IT team, you may have run into hesitancy or even resistance in getting definitive answers. For many IT teams, these questions require looking at cybersecurity risk in a new way. You may have discovered one of the most common mistakes companies make: assigning cybersecurity risk management to the Chief Information Officer. This approach can create problems for two reasons.



First, the CIO may not understand the business well enough to evaluate how important it is to safeguard the vulnerable information or technology. Smart firms recognize that the business owner has to get involved because only he or she knows what makes the business operate successfully. The IT team can serve as technical advisors to the business owner, but they cannot usually say what would happen to the business if the key competitive data, such as negotiation strategies or pricing policies, fell into the hands of a competitor. Without that knowledge, the IT team is unlikely to make a correct tradeoff between the costs of security and the costs of just accepting the risk as part of doing business.

Second, the CIO may not be evaluated on his or her security performance. Most CIOs are rewarded for getting technology to the users quickly and cheaply. In this environment, additional security becomes a financial cost that can also cause delays. The CIO’s investment in security is likely to be less than what is needed.

As a result, many firms are pulling the cybersecurity function out from under the CIO, and assigning that function to the organization’s chief risk management officer—who may also be the General Counsel (who is often responsible for compliance risk) or the Chief Financial Officer (who is often responsible for foreign exchange risk). At a minimum, there needs to be a conversation among senior management about how cybersecurity risk is assigned and the supervisory and reporting lines for that function.

Step Three: Staff for a Comprehensive Approach

Cybersecurity risk is not primarily a technology problem. It requires the involvement of other corporate functions including; human resources—to conduct personnel screening and employee training and awareness; physical security—to prevent theft or compromise by old-fashioned means; a public relations strategy—in case of an incident, legal and compliance expertise; and an understanding of the business value of the information that is being protected.

Best practice suggests forming a cross-disciplinary team to drive the strategy, ensure all aspects are considered and promote buy-in.

Step Four: Ensure Objectivity

Most CEOs do not have the time or expertise to objectively evaluate the performance of their cybersecurity team. Therefore, it is necessary, as with all risk management structures, to ensure that an independent team—that may be internal or external—validates and tests the measures that the cross-disciplinary cybersecurity team has put in place.