

Cyber attacks are reaching pandemic levels. State-sponsored groups and organized crime are successfully stealing valuable intellectual property—including product designs and military capabilities, critical infrastructure and operational readiness information, and businesses' and consumers' financial data—often without anyone realizing the attack has occurred. Losses from cyber attacks threaten the financial stability and competitive advantage of companies, government agencies, and nations. But preparedness cannot be delegated solely to the IT department. The involvement of the entire enterprise, armed with an understanding of the highly dynamic landscape, is vital for warding off potential threats.

## Understanding the Ever-Changing Cyber Security Landscape

PERSPECTIVES

An estimated 100 countries have developed cyber warfare capabilities, with the U.S., China, and Iran gathering particular media attention; and organized crime has created a global underground economy of hackers-for-hire to attack, steal, and monetize a company's proprietary information, take employee personal information, or disable operations. The incidence of attacks is actually much higher than is commonly thought, since many attacks are not reported to avoid bad publicity.

The situation is only worsening as adversaries aggressively invest in improving their attack capabilities. Consider the Aurora attacks on Google and other Fortune 500 companies, the Stuxnet malware targeting industrial control systems, and Iran's attacks on both governments and corporations. As these examples demonstrate, all types of organizations are susceptible.

To deal with this highly dynamic and asymmetric threat, many organizations continue to fund static, manual processes supported by investment in outdated technologies. Truly effective preparedness, however, requires an enterprise-wide approach that is based on an understanding of the highly dynamic landscape and is led by senior management.

### Understanding the Threats and Risks

The organization needs to understand the potential players, their motivation, and the financial impact of a successful attack. Cyber attacks are motivated by adversaries that want to: 1) steal critical or sensitive information, ranging from mission to personal, 2) impair or disable operations—product development, manufacturing, and so on, or 3) destroy or modify key information so that the organization makes incorrect decisions. Only a single weakness is needed for an attack to succeed.

### Taking an Enterprise-Wide Approach

In the past, executives would often delegate the problem to IT operations without understanding the risk model. Organizations must

stop thinking of cyber security as an IT problem exclusively. It is an enterprise risk, similar to physical, financial, and environmental threats, and, therefore, needs to be dealt with on an enterprise-wide basis. While the IT department is the steward of the information, only the information owners know the value of the information and the impact if it is compromised. As a result, the organization must have the skills to quantify both the probability of attack and the potential financial impact should an attack occur. These skills are critical for calculating what the optimal mitigation investment should be.

Investment in technical expertise will, of course, be required. The organization, however, needs to invest in human capital in many areas: policy, public relations, education/awareness, performance management, and organizational change management. Since many attacks target individuals to gain entry into the enterprise, awareness and communication efforts must reach all employees. As with pandemic flu awareness and prevention, the entire organization's involvement is necessary to combat cyber crime.

### Leading from the Top

In order for cyber security efforts to have real success, top management must lead the charge. The senior executive team needs to change how cyber security is managed, metrics are measured, and assets are protected. Only senior leaders can prioritize resiliency and mitigation actions to ensure the entire organization continuously and collaboratively assesses threats.

By understanding the changing landscape, by promoting enterprise-wide involvement, and by driving continuous review and improvement from the top, organizations will be best prepared to respond when a threat occurs. The question is no longer whether the cyber threat exists—it's whether an organization is able to respond when an attack does occur.

*To discuss this Perspective in more detail, please contact PRTM Manager David Etue (detue@prtm.com).*