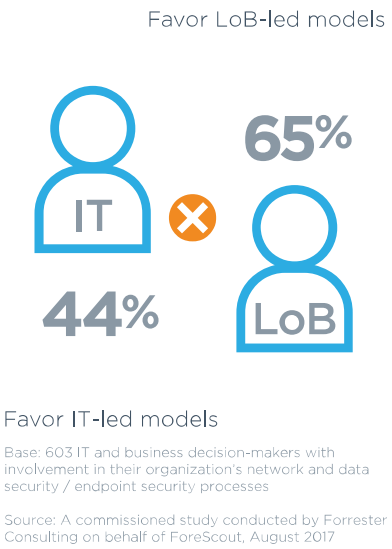
Improving Risk Assessment for IoT and Operational Infrastructure

Summary

The flood of new devices onto enterprise networks creates a network security challenge with technical, social and process components. These resources can help you start the risk assessment and management process:



- A study by Forrester Research reveals that security efforts often suffer from uncertainties in the division of responsibility between and Line of Business organizations.
- The Cybersecurity Framework offers a flexible, repeatable approach to security risk assessment and management that incorporates people, process and technology concerns to enable steady improvement in security and resilience.

One of the fastest-growing challenges for organizations is securing the billions of devices and operational technologies pouring onto enterprise networks. Organizations are harnessing these devices with new analytics, monitoring and control systems, creating new operational infrastructures that present irresistible strategic opportunities. However, without careful planning, these operational benefits can result in serious security issues: larger attack surfaces to protect, unknown vulnerabilities to avoid and unmanaged cybersecurity risks to prevent.

> Every aspect of business has risks that can be managed – and managed well. Cyber exposure is no different. — (Dark Reading, January 2018)

The Challenge

These emerging infrastructures expose organizations to significant operational risks and economic impacts. Consider a few recent examples:

- A.P. Moller-Maersk was hit by the June 2017 NotPetya malware attack. Five hundred locations were affected for up to two weeks, forcing three business units to shut down and causing an estimated revenue loss of US$ 300 million.

- NotPetya also affected pharmaceutical giant Merck, disrupting bulk ingredient manufacturing, product formulation and packaging operations, causing US$ 135 million in lost sales revenue and forcing management to revise Q3 investor guidance.
- In September 2016, the Mirai botnet, a massive global network of compromised home security and entertainment devices, launched the largest traffic flood ever recorded (620 Gbps) against KrebsOnSecurity.com, a popular security website. Akamai, the site's pro bono host, was eventually forced to withdraw support due to unsustainably high costs

This can lead to incomplete data in asset inventories and out-of-date information in configuration management databases (CMDBs). As a result, organizations may also be unaware of the additional attack surface and elevated risks from these endpoints.

Despite ever-increasingly sophisticated technology and methods, the answer to this exposure and risk may be in using a fundamental approach to network and device security. Also, there is a growing body of evidence that suggests some missing elements may be social and organizational, not technical.

Organizational Vulnerabilities, Operational Risks

To ensure the cybersecurity of and operational infrastructure, enterprises should understand the roots of vulnerability. ForeScout commissioned Forrester Research to investigate the challenges inherent in securing networks subject to large influxes of devices. In August 2017, Forrester surveyed 603 and Line of Business (LOB) decision makers. Key findings include:

- Cybersecurity responsibility is poorly defined: Line of Business organizations increasingly deploy and configure both traditional and operational technologies, including devices. Opinions vary on who is responsible for their security: respondents favored -led models, while LOB respondents favored LOB-led models. Not surprisingly, gaps in accountability often ensue.
- Overconfidence is widespread: 70 percent of respondents felt confident their networks were secure. When challenged in an audit, however, only 18 percent remained confident they could identify 100 percent of -connected devices on their networks.
- Risk tolerance is excessive: 59 percent of respondents were willing to accept medium to high risk in their security compliance which was surprisingly high.

The Solution: Follow a Framework

Because infrastructure is vulnerable to risks arising from technology, people and process, we need a structured framework for identifying, evaluating and prioritizing risks, designing security measures, responding to attacks and restoring normal operations. While it isn't obvious to look to the government for ideas, just such a framework is ready at hand. The U.S. National Institute of Standards and Technology () Cybersecurity Framework enables organizations of any size, degree of risk exposure or technical sophistication to apply the principles and best practices of risk management to improving security and resilience.

The core of the frameworks is a set of five concurrent and continuous functions: identify, protect, detect, respond and recover (see the sidebar). These functions prompt an organization to identify the

parties responsible for planning and implementing security measures and recovery activities. This risk assessment model can help address many of the issues highlighted in the Forrester paper.

The Cybersecurity Framework Core: Five Functions

Identify – Assess the risks associated with systems, people, data and process within the business context as a basis for prioritization and resource allocation.
Protect – Develop and implement appropriate safeguards to secure critical infrastructure services and limit the impact of a potential security event.
Detect – Develop and implement appropriate activities to enable the timely and accurate discovery of a security event.
Respond – Develop and implement appropriate actions to manage and contain the impact of security events.
Recover – Develop and implement plans to restore the operational capabilities or services impaired by a security incident.

Success in Cybersecurity and Risk Management Starts with a Plan

Securing devices and operational technologies may be more complicated than locking down desktops and servers, but the tools we need to succeed are readily available and complacency is our greatest risk. An excellent starting point is to download the Forrester report: Fail to Plan, Plan to Fail and the Cybersecurity Framework. By applying a structured planning framework to the full range of cyber vulnerabilities—people, process and technology—we can steadily improve the security and resilience of all our critical infrastructures.