ActualTech Media

UncommonX

The Business Case for Security

Lawrence Miller

CONTENTS

Recognizing That Security Is a Business Problem 2

Putting Security into Business Terms 2

Threats Are More Sophisticated; Security Is More Complex 3

Get Strategic with Your Security 4

IN THIS PAPER

Discover how small and midsize businesses can reduce risk and implement enterprise-class security—without the cost and complexity of enterprise security operations.

Highlights include:

- Recognizing security is a business problem
- Threats are more sophisticated and security is more complex than ever before
- Technology alone is not the answer

Recognizing That Security Is a Business Problem

Ransomware attacks are nothing new. But ransomware—and cyberattacks in general—once again landed in the spotlight in 2021 thanks to high-profile attacks against major corporations like Colonial Pipeline and JBS. The success of attacks such as these, and the increasing willingness of victims to pay ransom demands, further emboldens threat actors. As a result, devastating cyberattacks will continue to multiply in scale and frequency and become more disruptive to businesses and our everyday lives.

Media reporting about these recent incidents tended to focus on the compromise of massive amounts of sensitive data (financial records, personally identifiable information, or protected health information) and the associated costs (penalties, fines, lawsuits, customer notification, credit monitoring services, and brand reputation damage).

> **Devastating cyberattacks will continue to multiply in scale and frequency and become more disruptive to businesses and our everyday lives.**

What became even clearer through the reports was just how vulnerable business operations are to breaches and other forms of cyberattack. Despite being able to restore their critical systems and data within a matter of days—no small feat—both companies had their business operations effectively shut down by these attacks. That caused ripple effects that reached across their supply chains and even directly impacted individual consumers.

And ransomware isn't just a problem for large enterprises. A ransomware attack targeting the software supply chain of Kaseya VSA in July 2021 compromised as many as 1,500 small businesses, making it one of the largest ransomware attacks to date. Thus, small and midsize businesses must address the same threats as larger enterprises—but without the vast in-house resources of large enterprises.

Putting Security into Business Terms

While the heads of IT and security departments understand the true threat of cyberattacks, other leaders in their companies may not. Some business leaders have become more astute with regard to security issues, but their native tongue is still "business." With that in mind, security and network executives like yourself need to put security into business terms if you want to convince decision makers that security is a critical issue they must address.

You'll get a lot more attention from product development managers if you tell them they risk a six-month delay on a new product launch due to key R&D being lost in a ransomware attack. And plant managers will certainly understand what a distributed denial-of-service (DDoS) attack means to business operations if you tell them their production line could shut down.

You need to offer these business leaders a modern approach to security that provides accurate and timely insights in a context-relevant vernacular they understand. Give them answers that will help them confidently manage the business through whatever risks they're facing. The following will help you do that.

BUSINESS DRIVERS

Businesses today are realizing remarkable new opportunities and reimagining entire industry business models through their digital transformation initiatives. Security must be an integral part of these initiatives to ensure the company can achieve its goals while also minimizing risk.

Security is often perceived as a business inhibitor, but done correctly, security safely enables the business, increases agility, and can be a real market differentiator. Instead of security being a separate entity whose activities are disconnected from normal network operations, it

needs to be an integrated part of your IT operations. That is, IT done securely rather than security being a separate IT function.

VULNERABILITY AND RISK ANALYSIS

The U.S. National Institute of Standards and Technology (NIST) developed a Cybersecurity Framework that offers companies a risk-based approach to manage cybersecurity risk while they pursue their business objectives. It's a flexible and intuitive process built on five core functions of cybersecurity: Identify, Protect, Detect, Respond, and Recover.

The Cybersecurity Framework addresses the importance of knowing what you're protecting (that's asset management) and identifying threats, vulnerabilities, likelihoods, business impacts, and prioritized risk responses (also known as risk analysis).

RISK MANAGEMENT

To survive, businesses must continuously identify, assess, and respond to risk based on changing business conditions and the rapidly evolving threat landscape. An effective risk-management program helps ensure businesses understand their risk and can make informed business-centric decisions about cybersecurity investments and activities.

Risk management marries the results of vulnerability and risk analysis to your cybersecurity investments and activities. It's an ongoing process that ensures your business can quickly and effectively adapt to a changing risk profile.

Threats Are More Sophisticated; Security Is More Complex

Most businesses struggle in the face of advancing threats. They don't know what to do, don't understand the threat, and don't know how to get that understanding. So, they inevitably buy more security tools, looking for a solution that they hope will give them all the answers or helps them minimally meet government compliance requirements. However, this approach just compounds the risks and complexities for businesses.

TECHNOLOGY ALONE IS NOT THE ANSWER

Too often, IT and security leaders make the mistake of thinking that the right technology investments will solve their security challenges. They wind up with a glut of security tools and "black boxes," some of which they don't even need. Indeed, according to Momentum Cyber's "Cybersecurity Almanac," there are more than 3,000 security tools on the market. Loading up on tools often leads to potentially serious consequences for businesses, including:

- **Alert overload,** due to overwhelming amounts of data and alerts being generated by tools—only 7% of alerts are responded to today
- **Delayed response,** due to a lack of integration and the kind of automation that could help prioritize risk and identify false positives in real time
- **Greater risk,** due to improper management, lack of optimization, and misconfiguration of tools
- **Overspending,** due to redundant functionality across different tools

BUILD A PLAN BASED ON DEFENSE IN DEPTH

Defense in depth is a proven security axiom that helps to ensure that threat actors don't get the "keys to the castle" by simply defeating a single security solution, such as a firewall or anti-malware protection (see **Figure 1**). An effective defense in depth strategy ensures protection across a broad spectrum of risks. Organizations today leverage a wide array of security solutions to achieve defense in depth, from extended detection and response (XDR) and next-generation firewalls (NGFWs), to cloud access security brokers (CASBs) and security orchestration, automation, and response (SOAR).

> **Your technology investments should be determined by your evolving business and operational capabilities.**

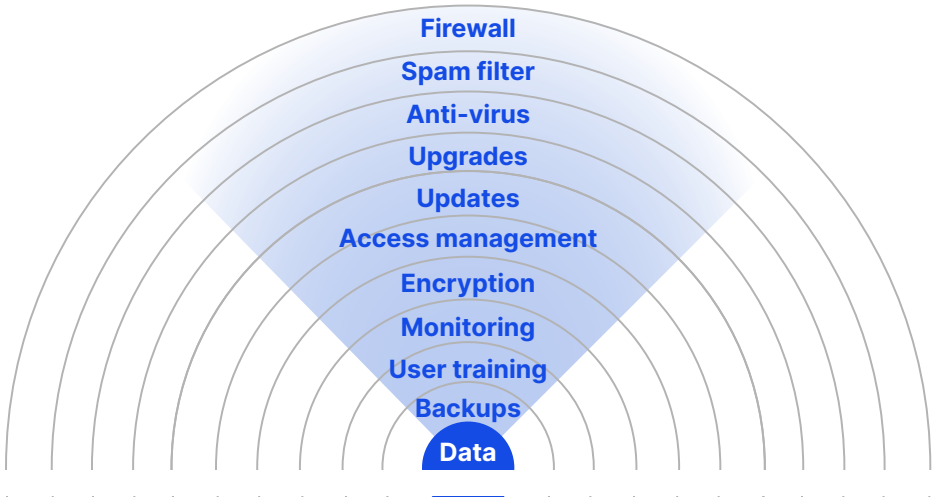

Figure 1: The many layers that make up a defense in depth security strategy

Some or all of these security solutions may be part of an enterprise security fabric that delivers comprehensive protection to the business. When building a defense in depth strategy, it's important to be proactive and plan your investments. Don't just allow your security environment to evolve (and sprawl) over time. Your technology investments should be determined by your evolving business and operational capabilities.

ADDRESS PEOPLE, PROCESSES, AND TECHNOLOGY NEEDS

Effective cybersecurity requires a balanced approach that addresses the people, processes, and technology needs of the business.

Security technology gets more and more advanced every year and it requires highly trained people to operate it. The problem is that there's a shortage of skilled security professionals globally. For smaller businesses, it's a daunting and possibly insurmountable challenge to build and retain an effective security team that can handle all aspects of security operations, management, and incident response. Larger companies may be able to fully staff a 24/7/365 Security Operations Center (SOC) with security architects and engineers, yet they still have the same challenges facing every other business: alert overload, siloed tools, and technical complexity. Simplifying security and aggregating it with network operations is crucial to a seamless and continuous communication infrastructure, which will help eliminate redundant tools and reduce the need for scarce skillsets.

Likewise, ensuring that security processes and workflows are both effective and efficient is no small order. Incident response, business continuity, and disaster recovery are key processes that must be routinely reviewed, regularly tested, and continuously improved in relation to changing business objectives and operational processes.

Finally, the technical solutions that you invest in and deploy must address your risk posture. They have to integrate with your existing security solutions as much as possible. They must maximize limited staff resources with automation and artificial intelligence (AI). And it's essential that they demonstrate a tangible return on investment (ROI) and a business-centric approach to security that enables the organization to achieve its business objectives while minimizing risk.

Get Strategic with Your Security

UncommonX offers unmatched enterprise-class cybersecurity protection for mid-size organizations by combining adaptive threat and intelligence software with 24/7 industry experts, making it easy to constantly both map and fix root causes of security vulnerabilities. Taking a market-first inside-out approach to ongoing digital security risks through unique curated threat feeds and automated analytics, the UncommonX BOSS intelligent security platform provides clear contextual awareness to yield accelerated outcomes to mitigate and guard against threats.