6 Benefits of Cyber Security – Defending Against Cyber Attacks



ARTICLE 03.15.22 GUI COZZI

As a business leader, the need to seek the next competitive advantage has always come with the keys to the corner office. Today, one of those advantages can come in a surprising form: cyber security.

On its surface, the subject of cyber security may be considered solely as a defensive position. Or even a “wait and see” tactic, with organizations adopting upgraded technologies or outside expertise after the fact, incident-by-incident.

This has been particularly true for small to midsize businesses, many of which have considered the cost of proactive cyber security too great. Or they may consider their operation simply too small for cyber criminals to target. But as the world now knows, that’s not the case: 43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves. And in the end, this has resulted in significant blows to their bottom lines and their reputations.

So as customers become more attuned to the impact of cyber security threats to their own data, the **business benefits of cyber security** are coming into focus. Savvy leaders are making cyber security a priority to not only help **mitigate risks,** but also **boost brand trust, ensure compliance, increase productivity** — even **spark innovation**. All of which can help separate one business from the rest.

Top Cyber Security Focuses Today

The sudden shift to remote work took the world by storm. Now, more devices connected from more locations have created a continually expanding attack surface for cyber criminals to exploit. So the need to protect computers, mobile devices, servers, and the cloud is greater than ever — from every endpoint to anywhere sensitive data travels.

A thorough strategy for businesses of any size includes multiple levels of protection utilizing a range of products from different sources. In a recent cyber security FAQs post we cover the different **types of cyber security** businesses implement to mitigate cyber threats, including **network security**.

Network security, in general terms, refers to the layers of technologies, devices, and processes designed to protect your network and vital data from breaches, intrusions, and other threats.

A network firewall that can control traffic based on security settings and permissions is typically at the top of every list. But because an attack can occur at any layer, a robust approach should address additional key elements in the network, including:

- **Hardware:** Secure employee devices to ensure they're safe to use, and present minimal risk if stolen or compromised. Restrict access to routers and cabling. And keep all hardware up to date. Outdated hardware may not support the most current software security upgrades, and can also inhibit your team's response to cyber attacks.
- **Software:** Install antivirus and antispyware software to protect against a range of malware that can compromise the network. Update all software and apps as soon as the newest version is available to add new features, fix known bugs, and upgrade security.
- **Security Processes:** Minimize your network's exposure to unauthorized access by adopting company wide policies and procedures. Include the use of a Virtual Private Network (VPN), and secure file sharing with encrypted files in transit and at rest. Create reporting and mitigation processes in the event of a data breach — and be sure to consider your data backup plan as well.
- **Access:** Adopt a zero-trust approach, assuming that bad actors are actively trying to break into your system. Authenticate every access request, and enable multi-factor authentication beyond username and password to verify who is accessing accounts.
- **Training:** Implement cyber security training for internal teams to understand their role in device security, network responsibilities, and how to identify signs of malicious activity.

Benefits of Investing in Cyber Security

At its core, cyber security is about risk management. But leaders who see the opportunities beyond just preventing data breaches and minimizing cyber threats can begin to realize the full potential and benefits that cyber security can bring to a business.

1. Protection against external threats

Millions of cyber threats are being created every year and at great cost to businesses, exceeding $1 trillion in 2020 alone.

While primarily launched for financial gain, the reasons behind cyber attacks can be as varied as the perpetrators themselves. Whether it's cyber criminals, hacktivists, or industrial spies, the common ground these bad actors share is how agile, sophisticated, and stealthy their attacks are becoming.

However, **a robust cyber security posture** that accounts for regularly-updated software can help organizations detect and respond to the methods, devices, and entry points being exploited, including:

- IoT devices
- Cloud and remote service attacks
- Fileless attacks
- Artificial Intelligence
- Supply chain attacks
- Social engineering
- Malware
- Man-in-the-middle (MitM)
- Denial of service
- Domain name system attack
- SQL injection
- Advanced Persistent Threats (ATPs)
- Zero day exploits

For a deeper dive into the sources and types of emerging threats facing businesses, be sure to check out our recent post on the Top Cyber Security Threats Today.

2. Protection against internal threats

The weakest link in the cyber security chain remains the human factor. Whether it's **accidental, negligent,** or outright **malicious,** insider threats can come from current or former employees, third party vendors, or even

trusted partners.

What's more, the exponential growth of remote work, personal devices used for business applications, and even IoT devices in remote settings can help these types of threats fly under the radar until it's too late.

But with proactive monitoring of networks and managed access, detecting and responding to threats can cut down on costly incidents. Moreover, providing consistent, up-to-date training can help turn the risk your people currently are into the extension of the cyber security solution you need.

3. Regulation compliance

In response to the increased cyber threats and exposure of sensitive data businesses face today, many regulatory bodies are setting standards to help protect organizations and their customers alike. Some of these regulatory standards include GDPR, HIPAA, PCI DDS, and SOX to name a few.

For industries that still remain underregulated, there's opportunity for businesses to invest in cyber security and see compliance as more than an obligation.

In fact, according to data privacy and cyber security law expert Jamal Hartenstein, leaders could approach cyber security in regulatory compliance as "a competitive advantage, getting ahead of industry competition before underregulated industries become regulated."

4. Improved productivity

Viruses and other cyber attacks can slow networks and personal devices down to a crawl, making it virtually impossible for employees to work. For websites to function. And for business to operate.

By implementing a range of cyber security measures — such as improved firewalls, virus scanning and automated backups — you can drastically reduce violations and the downtime it takes to remedy the breach. Education and training can also help guide employees to identifying potential email phishing scams, suspect links, and other nefarious criminal efforts.

5. Cost savings and value

According to the Hiscox Cyber Readiness Report 2021, the average cost of a single cyber attack to a small business in the U.S. is $25,612. Considering the fact that only about 40% of SMBs operate at a profit — the loss of data and cost to recover it, downtime to restart operations, and hefty fines can be a steep price to pay.

As cyber attacks only continue to grow more sophisticated and complex every day, it's important to weigh the cost of dealing with one attack versus the value of taking preventative measures. By mitigating risks, you put your business in a better position to respond, recover, and keep existing customers happy — a far more cost-efficient option than attracting new ones.

6. Brand trust and reputation

Perhaps the greatest case to make for the benefits of cyber security in business is the reputation that you earn. And keep.

One of the most important factors in business growth is customer retention. Maintaining brand loyalty through a strong cyber security position is paramount for customers today, and the shortest path to repeat business, recommendations, and higher per-ticket purchases.

It also opens doors to potential future ventures and expansion, helping producers land on the vendor list with larger organizations as part of their supply chain — that are only as strong as their weakest link. According to the National Institute of Information Technology (NIST), the factors that allow for low cost interoperability and rapid innovation also increase the risk of compromise. With so many high-profile cyber breaches in the past two years alone, larger companies are examining closely the cyber security practices of third-party vendors.

Start with a Cyber Security Audit

Fact is, as cyber threats evolve so do cyber security solutions. But knowing where you stand today can help guide where you go tomorrow.

With a **cyber security audit**, you get a comprehensive, independent analysis of your current cyber security posture. It can identify vulnerabilities, expose weaknesses and high-risk practices, mitigate the risk of attacks, and continue to foster confidence and trust with your key stakeholders and customers alike.

Once issues are identified, strategic measures can be put in place to increase real-time visibility across your network and devices, and improve your team's ability to react in the event a breach occurs.

Stay Safe, Secure, and Ready to Succeed

When viewed through the lens of expense alone, the full suite of business benefits cyber security can offer may not be immediately evident.

But the fact is, cyber security is no longer considered another line item that's simply part of doing business. It's beyond being an IT issue. An effective cyber security strategy is a growth strategy, a priority launch pad for innovation, and a point of differentiation from the competition.

While there's no way to be 100% protected against cyber attacks, a proactive approach to enhancing your strategy shows a commitment to your customers, their data, and your reputation.

Mitigate risks, safeguard valuable data, and assess your current cyber security stance. Connect with Dean Dorton for a cyber security assessment today.

And for more insights and analysis on trends and cyber security solutions, be sure to subscribe to our blog.