

The Foundations of Cybersecurity for Digital Commerce

Digital commerce is the buying and selling of goods and services via Internet-connected channels such as commerce infrastructure and mobile networks. It also includes the people, processes, technologies, and marketing activities to support online transactions.

These various aspects of digital commerce require security measures to ensure customers feel safe and confident during the entire shopping experience. In today's increasingly interconnected digital world, security and customer confidence must also include all aspects of commerce infrastructure including payment and fulfillment.

> The pandemic brought a rush to implement new digital commerce solutions, but rapid adoption also increased cybersecurity and privacy risks.

How big of a problem is cybercrime?

Digital reliance during the pandemic has driven cybercrime up 600%.¹ To address pandemic-related changes in their businesses, 91% of organizations plan to increase cybersecurity spending in 2021 and beyond.²

Defending against cybercrime requires constant vigilance against new attacks and increasingly sophisticated threats.

What types of attacks and threats happen most often?

- **Internal threats:** Cybercriminals use social engineering to obtain access to high-level accounts or gain insider long-term financial trust.
- **Third-party compromises:** Intruders obtain access to supplier systems, partners, or vendors so they can infiltrate your systems.
- **Ransomware breaches:** Cybercriminals with longer-term access tailor their ransomware code specific to your data and environment. An attack can be activated within seconds of access.

How is cybercrime changing?

Cybercriminals are finding new ways to take advantage of our increased reliance on Internet-based services. Specifically, cyber attacks are increasingly targeted and automated, taking advantage of the power and automation of cloud computing and previously compromised systems and networks.

Account takeovers are a popular method used by attackers to gain access and control customer and business data. Ransomware incidents are also becoming more prevalent and sophisticated, often involving theft (or threat of theft) of Personally Identifiable Information about organizations and their customers. In fact, a ransomware attack occurs every 10 seconds.³

What's the cost of cybercrime?

The time and money needed to address a data breach can be immense. **The average cost of a data breach in 2020 was \$3.86 million.**⁴

Successful cyberattacks can also lead to revenue loss due to the disruption of digital commerce channels. Damage to brand reputation and consumer trust is also apparent if people don't feel safe in completing transactions and sharing information online.

To fight back, companies must work to secure their environments and data with four critical steps:



Anticipate



Monitor



Protect



Respond

The average cost was \$1.07 million higher in breaches where remote work was a factor in causing the breach⁵

Customer PII cost an average of \$180 per lost or stolen record in 2021. In 2020, customer PII cost \$150 per lost or stolen record, representing an increase of 20%.⁵

Four Steps to Cybersecurity

1. Anticipate -

Understanding how your digital commerce ecosystem may be susceptible to cyber attacks is critical to building an effective cybersecurity program. This includes vulnerabilities in the specific software or cloud infrastructure in use; integration with business partners; how customer access is controlled; and how all of the systems are managed and monitored. Develop a Threat Intelligence program to maintain awareness of technical vulnerabilities as well as current industry-specific threats such as payment security, fraud techniques (returns, loyalty programs), 3rd party integration risks, data privacy risks, and other compliance-related concerns. Automation should be leveraged to proactively identify priority items for your cybersecurity team to investigate. Where possible, leverage automation to proactively block cyber attacks and/or modify system or user access to eliminate or reduce the impact of a cyber attack.

2. Protect -

Start by protecting your web applications from risk and vulnerability. Remember that cybercriminals have become advanced in how they exploit your web applications. They can attack anything – from URLs and applications to product uploads or attachments – while they attempt to circumvent your security measurements and expose your weaknesses.

Another way to protect your business is from within. Look closer at the internal use of resources, and ensure only the right users have appropriate access. Ensure all users participate in security awareness training, with focused training for critical developer and operational


positions. Don't forget, executives are often the targets of social engineering attacks aimed at gaining access to highly sensitive information or exploiting financial gains.

Review 3rd parties and business partners whose systems interact with your organization to determine what types of information are stored, transmitted or transacted - and review to ensure that controls meet or exceed your minimum requirements for data security and privacy.

3. Monitor -

Identify your business critical systems and monitor network traffic, user behaviour, application / data access, and any other critical control points for suspicious activity or policy violations. Leverage automation (emerging AI and Machine Learning technologies) to identify patterns, anomalies, and eliminate false positives. If your organization develops and hosts its own software, implement continuous review of code and secure development practices. If your organization relies on 3rd parties, obtain assurance that their processes undergo rigorous review. Monitoring efforts

should also serve your organization's industry and regulatory compliance and reporting requirements. Most importantly, if your organization does not have the in-house capabilities, consider engaging a Cybersecurity Service Provider who has specialized knowledge and experience in securing digital commerce solutions.

The majority of successful breaches exploit at least one system that has not been updated. Patching and software updates are a critical component of maintaining resilience to cyber attacks. 

4. Respond -

When an indicator of compromise is suspected or discovered, it is critical to respond immediately. Cyber attacks are often highly automated, and once launched are difficult to contain, so early detection of suspicious activity or anomalies using automated cybersecurity systems is essential. Many organizations will require help from a specialized breach investigation and recovery firm to ensure all attack points are secured and that no evidence of data leakage and/or privacy breach is found. In confirmed breach scenarios, it is important to restore the confidence and trust of your customers. Working with industry experts can ensure the correct information is disclosed and proper remediation steps are followed. After every incident (suspected or real), review the processes that were undertaken to investigate the incident and factors that might reduce the likelihood of future breaches.

80%
Cost difference where
security AI and automation
was fully deployed
vs. not deployed⁵

How can a Cybersecurity Service Provider (CSP) help?

The fast-evolving landscape of cyber threats requires businesses to establish a stronger, more agile security posture. Organizations either need to hire, train, and maintain a team of experts to implement their security practice, – or hire 3rd party experts for some or all of their cybersecurity needs.

Many organizations choose to focus resources on their core business, and turn to traditional Managed Security Service Providers (MSSPs) to manage and monitor their security infrastructure, including devices and systems. MSSPs typically provide services such as intrusion protection, firewall management, vulnerability scanning, and anti-virus services.

What are some risks to consider?

While MSSPs give organizations additional peace of mind in the fight against cyber threats, they often lack contextual awareness of the industry-specific threats their clients need protection against. MSSP lack of industry focus results in a visibility gap pertaining to specific threats and risks faced by their customers. This is one factor in the persistence of cyber breaches across multiple industries.

Meet a solution for the modern era of cybersecurity

Today's businesses need more focus on cybersecurity from their digital commerce partner. They need a partner that understands the industry-specific cybersecurity needs of the digital commerce space.

That's where Pivotree is different:

- As a commerce-focused company, Pivotree delivers domain-specific expertise and visibility.
- We are uniquely positioned to fully manage the risks, compliance, and governance of your digital commerce ecosystem (applications, cloud services, user access, etc.).
- Pivotree's Cybersecurity solutions make use of highly automated techniques to proactively manage cyber threats - and in many cases, prevent breaches before they occur.
- We offer a foundational solution for holistic cybersecurity: Pivotree Cybersecurity Watch.

The average
total cost of a
data breach
increased by
nearly
10%
year over
year⁵

How does Pivotree Cybersecurity Watch work?

Pivotree Cybersecurity Watch leverages best in breed technologies – combined with a team of security experts at Pivotree – to protect and defend your digital business against evolving cyber threats.

Benefits:

1

Best-of-breed technologies:

No piecemeal approach here. We've selected the best-of-breed technologies, integrating them together under a single ecosystem backed by our people, processes, and expertise.

2

Digital commerce expertise and visibility:

Because we manage customer environments and the security solution, we can take immediate action to avoid a successful attack. Plus, if we see any indication that more than one customer is under attack, we can take action to stop breaches before they become an issue.

3

No more hidden costs:

We help you avoid the hidden costs of cyberattacks, such as: fines, the damage done to your brand and reputation, or the loss in revenue when your site goes down (potentially during peak traffic times) and more.

4

A frictionless experience:

Trust is a core pillar of frictionless digital commerce. If your customer doesn't trust your site – or if it's down from an attack – that's friction. Cybersecurity Watch helps your site stand out as the easy choice. Customers know they can trust shopping and completing transactions with your brand.

Cybercrime is rising – but not on our Watch.



Learn more at our webinar:
**The Foundations of Cybersecurity
for Digital Commerce**

October 26 at 1:00 PM CDT

CLICK HERE TO REGISTER

Pivotree is a leader in frictionless commerce with expertise in eCommerce, MDM, Cloud, Cybersecurity, and Supply Chain solutions. Supporting clients from strategy, platform selection, deployment, and hosting through to ongoing support. Leading and innovative clients rely on Pivotree's deep expertise to choose enterprise-proven solutions and design, build, and connect critical systems to run smoothly at defining moments in a commerce business. Pivotree serves as a trusted partner to over 170 market-leading brands and forward-thinking B2C and B2B companies, including many companies in the Fortune 1000.

¹ The Latest: UN warns cybercrime on rise during pandemic, The Associated Press, May 23, 2020, <https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542>.

² 78% Lack Confidence in Their Company's Cybersecurity Posture, Prompting 91% to Increase 2021 Budgets, February 24, 2021, <https://finance.yahoo.com/news/78-lack-confidence-company-cybersecurity-153000182.html?guccounter=1>.

³ Muncaster, Phil, One Ransomware Victim Every 10 Seconds in 2020, February 25, 2021, <https://www.infosecurity-magazine.com/news/one-ransomware-victim-every-10/>.

⁴ Nead, Nate, How To Prevent A Data Breach in Your Company, July 30, 2021, <https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=46d5e1c18da7>.

⁵ Cost of a Data Breach Report 2021, IBM Security, <https://www.ibm.com/security/data-breach>