Visa
Economic
Empowerment
Institute

Imagining an Open
Future for Payments

Keeping the lights on for small businesses: Safeguarding the payments ecosystem during the pandemic

ERIN ENGLISH AND JONATHAN DAVIS / DECEMBER 2020

Insights

- Cyber-threat actors are making the most of the pandemic and the vulnerability of small businesses. This sudden change has expanded the surface area exposed to a cyberattack, creating new opportunities for cybercriminals.
- Regulations help enterprises meet a baseline level of cybersecurity protection, which, from the regulators' perspective, helps realize a level of systemic protection for an entire market. However, regulators still struggle to coordinate and harmonize rules and regulations globally, even though the cyber-threat is an international one.
- Governments can create a more enabling policy environment so that global networks can align cybersecurity best practices across jurisdictions and bring innovations to market faster. Governments play a key role in ensuring a cybersecurity policy environment that promotes a flexible, risk-based approach to cybersecurity.

The COVID-19 pandemic has accelerated digital transformation and changed the nature of commerce. This shift in consumer behavior has forced enterprises of all sizes to reinvent how they conduct business, and millions of small businesses have had to find new channels with which they can connect with customers. These businesses are racing to launch or expand their digital infrastructures in response to the pandemic—many are opening e-commerce channels or going online for the first time. Simultaneously, employees with access to sensitive business and customer information are frequently working in new, less secure territory—their homes. This sudden change has expanded the surface area exposed to a cyberattack, creating new opportunities for cybercriminals. According to an October 2020 Ponemon survey, 71 percent of companies believe teleworkers are putting their organization at risk of a data breach, and only 46 percent believe they are effective in reducing the cyber risk brought on by remote work.

Cyber-threat actors are making the most of the current crisis and the vulnerability of small businesses. Now, as governments and businesses are looking to revitalize their local economies by supporting online access to goods, services, and information, it is critical that organizations of all sizes remain vigilant and take steps to ensure the appropriate level of cyber resilience. Every day in our increasingly connected economy, there are new market participants, all with varying degrees of cyber maturity. These additional players are involved in a growing number of transactions, and they process significant amounts of sensitive data. Brand-new or rapidly expanding digital businesses have the potential to introduce significant risks into the wider payments ecosystem. That is why it is important for them to establish a baseline level of cybersecurity best practices. To protect economic recovery for small businesses and encourage sustainable growth, established companies such as Visa have a responsibility to share cybersecurity best practices and to help ensure the cyber resilience of the wider payments ecosystem.

The current state of the threat environment

Almost as soon as the pandemic began to alter the nature of work, businesses had to manage heavier workloads, often with reduced staff, all while relying on new platforms. Cybercriminals wasted little time exploiting these changes. According to a Microsoft cybersecurity study released in September 2020, criminals began reducing their "dwell time," or the time they were taking between compromising a network and executing a malicious act such as stealing data or holding data ransom. This could mean cyber-attackers believed that there would be an increased willingness to pay as a result of an attack. Even before the pandemic, small businesses and underfunded governments were frequent targets of ransomware, with devastating consequences. According to a Cisco cybersecurity report in 2020, the paper revealed that ransomware was the most destructive threat for small and enterprise organizations with respect to downtime. Without adequate resources, precious time can be spent just assessing the extent of damage and restoring backups. Indeed, small businesses are likely to have longer downtimes following a security incident (five to 16 hours) than larger organizations (zero to four hours).

Cybercriminals must always innovate in response to hardened networks, new patches, and other cyber risk management procedures. However, these threat actors will still use past techniques against less mature organizations with poor or outdated cyber risk management practices. In a detailed report analyzing the COVID-19 data breach landscape, Verizon learned, "given that these tactics [cyber-threat techniques] worked before COVID-19, and that one of the results of the pandemic is that we have unwittingly provided a larger attack surface for those attacks, there is not much need for attackers to dream up new strategies and tactics to commit new crime."

Fragmentation of cybersecurity regulations in financial services is also a risk

One way for policymakers to help combat this risk is by requiring regulated entities to adhere to a set of cybersecurity best practices and procedures. Industry and regulators have a common objective: to ensure the resilience of the financial services sector and protect it against cyber-threats. Regulations help enterprises meet a baseline level of cybersecurity protection, which, from the regulators' perspective, helps realize a level of systemic protection for an entire market. However, regulators still struggle to coordinate and harmonize rules and regulations globally, even though the cyber-threat is an international one. The World Economic Forum highlighted this problem in a report that includes recommendations to improve the cybersecurity of fintechs, arguing that a lack of coherence across the private sector makes it difficult to apply resources in a rational manner. This is hardly a new problem, and is one that the financial services sector has often struggled to manage. According to a 2019 International Monetary Fund (IMF) report, "Financial firms are spending significant resources juggling regulatory demands and implementing the new rules. In some instances, regulations are overlapping, duplicative, and conflicting. The result, in some circumstances, is to absorb time that would be better spent building stronger defenses."

How Visa is securing the payments ecosystem

As a truly global company, Visa appreciates that the world is increasingly interconnected. Cybersecurity is a global issue, and threats can materialize from anywhere in the world, and from any point within a supply chain, with no regard for borders or jurisdictions. Organizations must manage cyber risk far beyond their own perimeters and understand the risks posed by trusted third parties and their connected systems. As more organizations adapt to enabling secure remote work options, whether in the short or long term, cybersecurity provides a key pillar for operational resilience. Successful navigation of any type of business disruption requires a strategic combination of planning, response, and recovery. To maintain cyber resiliency, an organization should regularly evaluate its risk posture, including its ability to operationally execute key processes through a combination of human efforts and technology products and services.

When managed effectively, the move toward an open payments ecosystem and interconnectedness between technology players and financial institutions is an effective means of maximizing innovation and financial inclusion. Critically, such a payments ecosystem can also increase insight into risks, and the means to remediate those risks quickly and at scale. This puts the emphasis on managing risks effectively, because without constant vigilance, a complex ecosystem can also increase cyber risk. Participation in global commerce relies on access to secure, trusted payments networks that can operate across borders. The payments chain and ecosystem are evolving rapidly, and this trend is set to continue over the coming years. At Visa, we are seeing not just an increase in volume of market participants who need to be cyber resilient, but also a rapid increase in the amount of data shared between these additional players. We see how new technology brings benefits, but also challenges, in terms of how to keep our networks and data safe.

Combating fraud is a global issue—criminal groups increasingly use sophisticated international syndicates to commit fraud across borders. Global networks are well positioned to detect and prevent fraud and apply global technologies and intelligence to mitigate local risks. Fraud detection relies on access to global data. It involves tracking and analyzing suspicious transactions across multiple countries. Companies can more effectively keep fraud rates down when they can check transactions against global patterns. Visa makes considerable investments to maintain a resilient network against an ever-changing cyber-threat landscape. Updating and maintaining our technology capabilities and risk management services is a priority. Cybersecurity teams across the globe constantly conduct responsible intelligence sharing, monitoring, detection, response, and investigation to ensure cyber resilience in order to protect our clients, cardholders, and merchants.

Cybersecurity guidelines for enterprises, particularly small businesses

The costs of disruption—and remediation—for all types of cyber risk continue to increase as organizations face highly motivated adversaries who are able to leverage significant resources against their targets. To meet these challenges, it is important to recognize that although cybersecurity has always been a game of speed, it is also a team sport. Consequently, there are commonsense best practices that enterprises, particularly small businesses, can use to help ensure their security, which contributes to the overall security of the payments ecosystem:

- Build a culture of cybersecurity. Enterprise leadership, whether it is a corporate board or a small business owner, sets the tone and culture for an organization as it builds a cyber risk management strategy. Executive commitment is the best way to ensure that cybersecurity is given appropriate priority and resourcing as companies develop and implement their strategies.
- Prepare a cyber incident response plan and train employees to implement it. Every minute and every action is critically important to restoring the enterprise's network while it is under an attack. The time to socialize cyber response plans is before an incident, not during one. As US President Dwight D. Eisenhower famously remarked: "Peacetime plans are of no particular value, but peacetime planning is indispensable."

- Develop foundational and comprehensive cybersecurity best practices chartered by corporate policies. They may not be glamorous, but good cyber hygiene practices such as constant secure development practices, patching of systems, use of strong authentication and encryption techniques, and continuous security monitoring provide critical protections.
- If you are a small business, consider applying the tenets of the US National Institute of Standards and Technology (NIST) cybersecurity framework: Identify, protect, detect, respond, and recover. Regardless of an organization's size, these principles provide an important framework for managing cyber risk. Understandably, building a comprehensive cybersecurity framework can be a challenge for a small business, which is why NIST has also provided an online resource for small businesses called the small business cybersecurity corner. The United States Cybersecurity and Infrastructure Security Agency (CISA) also provides several resources small businesses can use to improve their cyber risk management. Finally, the United Kingdom's National Cybersecurity Centre provides a small business cybersecurity guide with a set of easy, actionable steps for small businesses to help improve their cyber resilience.
- Manage cyber risk far beyond your own perimeters and understand the risks posed by trusted third parties and their connected systems. Organizations must manage the cyber risk in their supply chains in order to ensure that they are themselves trusted participants in other organizations' supply chains.

Cybersecurity recommendations for policymakers

Improving the payments ecosystem does not just involve what businesses can and should do, but also involves understanding the role of the public sector. Cybersecurity is a cooperative effort to protect businesses and the rest of society from a common threat. Policymakers are rightly concerned about the vulnerability of small businesses to cyberattacks and fraud. One area in which governments can work together with the private sector to protect against threats and enhance awareness of best practices is to help defeat cybercriminals and certain nation-states that target inexperienced employees. To best achieve this goal, governments can create a more enabling policy environment so that global networks and platforms can align cybersecurity and payments security practices across jurisdictions and bring innovations to market faster. Governments play a key role in ensuring a policy environment that promotes a flexible, risk-based approach to cybersecurity:

- Be flexible and allow room for companies to tailor defenses to their business needs. Given the ingenuity of hackers and the fast-changing nature of cyber-threats, it is vital that cyber defenses evolve quickly to keep ahead of potential attacks.
- Base guidelines on globally accepted standards. International standards form the backbone of the digital payments industry, enabling ubiquity by maximizing global interoperability and acceptance across digital payments systems.
- Allow businesses to determine data storage practices based on business requirements. Data is a linchpin of the modern global economy, with digital trade contributing to economic growth and development. Digital trade barriers, including data localization requirements, can have unintended consequences, potentially harming cybersecurity by introducing vulnerabilities into otherwise secure global systems.
- Encourage transparency and information-sharing regarding threats, vulnerabilities, and controls between government and private industry, among government agencies, and between governments of different nations. Governments can also lead in the investigation and prosecution of cybercriminals to help eliminate "safe havens," and facilitate public awareness of cybersecurity efforts.

Sources

Cisco (2020). "Cisco Cybersecurity Report Series 2020." https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

Doyle, S. et al. (2020). "Systems of Cyber Resilience: Secure and Trusted FinTech." World Economic Forum. https://www.weforum.org/reports/systems-of-cyber-resilience-secure-and-trusted-fintech

Microsoft Digital Defense Report. (2020) *Microsoft Security Team*. https://www.microsoft.com/en-us/download/confirmation.aspx?id=101738

Ponemon Institute (2020). https://start.keeper.io/2019-ponemon-report

Verizon (2020). "Verizon Data Breach Investigations Report." https://enterprise.verizon.com/resources/articles/analyzing-covid-19-data-breach-landscape/

Wilson, C., T. Gaidosch, F. Adelmann, and A. Morozova. Cybersecurity Risk Supervision. (2019). *International Monetary Fund, Monetary and Capital Markets Department*. https://www.imf.org/~/media/Files/Publications/DP/2019/English/CRSEA.ashx

About the Visa Economic Empowerment Institute

The VEEI is a non-partisan center of excellence for research and public-private dialogue established by Visa.

The VEEI's overarching mission is to promote public policies that empower individuals, small businesses, and economies. It produces research and insights that inform long-term policy within the global payments ecosystem. Visa established the VEEI as the next step in its ongoing work to remove barriers to economic empowerment and to create more inclusive, equitable economic opportunities for everyone, everywhere.

Visit: visaeconomicempowermentinstitute.org