Visa Consulting & Analytics (VCA)

Countering emerging cyber threats in payments

A guide for businesses to help prepare for and prevent online fraud and cybercrime

Once committed by loosely organized groups targeting small-scale targets, cybercrime — criminal activity committed online — is more recently being committed by the likes of skilled, well-resourced threat networks with larger-scale targets and access.

In the United States, losses related to internet fraud skyrocketed almost 300 percent from 2020–2023. Fraudulent activities, which may involve a personal or corporate data breach, payments-card fraud, phishing, identity theft, etc., inflicted nearly $34 billion in damages for victims.[1]

With recent advancements in generative artificial intelligence (gen AI), attacks are becoming increasingly sophisticated.

For today's cybercriminals targeting large business, a single vulnerability in the data infrastructure can be the open door to mass data breaches and leaks.

As with offline crime, cybercrime is constantly evolving to beat security measures. Cybercriminals are continuously finding ways to exploit new and emerging technologies such as AI, posing significant challenges to cybersecurity efforts. For example, AI-powered attacks have become more sophisticated and evasive. AI can be used to generate highly personalized and convincing phishing emails, making them harder to identify. By understanding these evolving threats, businesses can better prepare and strengthen their defenses against cybercrime.

With a surge in digital payments and emerging API-led open banking use cases, their potential attack surface has expanded considerably. In this paper, learn how cybercrime is evolving and how businesses can anticipate and implement strategic measures to prevent breaches.

Defining cybercrime in the payment space

Cybercrime is criminal activity where computers or the internet are the source, target, or place of a crime.

In a payments context, it covers any fraudulent activity that involves the targeting of digitally enabled payment systems and companies that operate in the payments ecosystem.

Cybercrime also includes, but is not limited to, the theft of payment credentials that are stored on or processed by computers and networks; the use of compromised payment credentials to conduct digital payments, such as e-commerce payments; and the use of digital payment systems to monetize other forms of fraud, such as ransom attacks or the theft of government disbursements.

1. FBI National Press Office. (2025, April 23). FBI releases annual internet crime report. FBI. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

Cybercrime is an evolving landscape

With the rapid uptick of ecommerce and the digitalization of daily data exchanges between consumers and institutions, cybercriminals are turning their efforts to the internet. Online fraudsters, whose efforts are now being magnified with artificial intelligence (AI), are deploying malware attacks with unprecedented speed and impact.

Cyber-fraud incidents typically include data breaches, ransomware attacks, and phishing scams. While these incidents are not all specific to payments, many have a payments-related dimension. This is either because payment businesses may be targeted for such attacks or because cybercriminals intend to use payment systems to monetize their profits.

Increasing quantity of online consumers and businesses

The rise in business and transactions conducted online creates more opportunities for virtual fraudsters. Global retail ecommerce sales reached approximately USD six trillion and projected to grow 31 percent in the coming years to nearly USD eight trillion by 2028.[2]

Emerging AI-empowered tactics

While offering powerful tools for protection, AI is simultaneously supercharging cybercrime. Attackers are using AI to create "deepfakes," to deploy adaptive malware against outdated cybersecurity systems, to automate large-scale attacks, and to create sophisticated synthetic identities.

Merging various data centers

In recent years, the global payments sector has been subject to a wave of mergers and acquisitions, which can create transitionary data vulnerabilities.

2. Global retail e-commerce sales 2022-2028, Statista Research Department, Apr 22, 2025 https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Three categories of threat

In evaluating the risk from cyber fraud, it can be useful to look at the issue through three lenses, which can help reveal vulnerabilities and point towards the most effective solutions.

People-related errors

People-related breaches are the most common type of security incident. Almost every successful attack can be traced back to a failure to follow protocols – like someone clicking on a dubious email link, failing to follow password guidance or, in some instances, collusion with cybercriminals (insider threat).

This also goes beyond employees and applies to vendors and third parties too, since they often have access to an organization's systems.

The human dimension is regarded as the weakest link, which requires constant attention – including the effective screening of new hires, training and messaging for all employees, and education and messaging for customers. Some organizations also employ "simulated threat" exercises to identify where gaps in training, process, or technology would strengthen defenses.

Process-related weaknesses

Globally uniform and unchanging processes can also become a vulnerability (with cybercriminals on the lookout for consistent processes, as well as consistent process anomalies). In addition, sometimes organizations have processes, but do not have a consistent policy in place, such as patch management.

The situation calls for several protections, such as source code analysis and validation, disciplined incident response services, behavioral analysis, impossible login analysis and system account health – with regular reviews and updates of all processes.

Technology-related gaps and exposures

Wherever monetary value is transferred, or payment credentials are collected, processed, stored or transmitted, there will always be risks. And, as more payments are now digital, the enabling technology is under constant scrutiny.

In today's landscape, every payment business should also consider themselves a technology business, and risk-management teams should have deep technology expertise. Organizations should prioritize safeguards including up-to-date threat intelligence, network segmentation and analysis, close monitoring and protection of endpoints, tokenization and biometric authentication.

Five emerging trends in payments cybercrime

These five cyberfraud trends have captured the attention of payments-business strategists:

TREND #1

AI-driven cyberattacks

(criminal activities utilizing AI capabilities)

AI-driven cyberattacks can be significantly faster, larger-scale, and more sophisticated than traditional attacks, making them harder to detect and counter. Virtual criminals are now commonly using the following tactics:

- **Sophisticated phishing campaigns.** AI is being used to generate highly convincing phishing emails, messages, and websites that can bypass traditional security filters. These attacks use natural language processing to create personalized content that mimics legitimate communications, making them much harder to detect
- **Automated vulnerability discovery.** AI tools are being deployed to scan systems for weaknesses more efficiently than manual methods. These automated systems can identify zero-day vulnerabilities and potential entry points in networks at unprecedented speeds
- **Deepfakes.** AI-generated audio or video content that mimics real individuals, used for fraud or misinformation. For instance, a $25M scam in Hong Kong where a finance worker was tricked by a deepfake executive[3]
- **Data poisoning.** Attackers corrupt AI training data, compromising system integrity, potentially causing misbehavior in applications like chatbots

Traditional defenses, such as signature-based antivirus software (which detects malware by comparing files to a database of known malicious signatures) and endpoint detection systems (which monitor devices like computers and smartphones for suspicious activity), are struggling to keep up with modern cyber threats. Despite 41 percent of organizations using these traditional tools, only 15 percent report feeling confident in their effectiveness against current threats.[3]

AI's ability to hide the origins of attacks makes it even more difficult to identify and attribute them to specific sources or individuals. This complexity adds another layer of challenge for cybersecurity efforts.

By understanding the limitations of traditional defenses and the advanced capabilities of AI-driven cyberattacks, businesses can better assess their security needs and explore more effective solutions.

The following defenses are becoming more commonplace and integral to many payments-related businesses' cybersecurity protocols:

- **AI-powered threat detection.** Use AI for real-time anomaly detection and behavioral analysis to identify unusual patterns, like unauthorized access or data exfiltration
- **Zero-trust architecture.** Enforce strict identity verification for all users and devices and grant them only the minimum level of access necessary to perform their tasks (known as least-privilege access)
- **Endpoint security upgrades.** Deploy AI-enhanced endpoint detection and response systems to counter adaptive malware and zero-day attacks
- **Employee training.** Conduct regular on spotting phishing and deepfakes; simulations reduce susceptibility
- **AI-model security.** Secure training datasets and use adversarial testing to prevent data poisoning; conduct periodic audits to identify vulnerabilities in AI systems prior to possible exploitation
- **Ensure that critical data is regularly backed up.** Store these backups in locations that are not accessible from the network to enhance security

3. Chen, H., & Magramo, K, February 4, 2024, Finance worker pays out $25 million after video call with Deepfake "chief financial officer." CNN, https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

TREND #2

Adaptive malware programs that evolve in real-time

Adaptive malware is a top cyber threat due to its ability to evolve in real-time, making it exceptionally hard to detect and neutralize.

Some AI-powered malware programs, like BlackMamba, are adaptive—meaning they dynamically alter their codes, patterns, or attack methods in real-time to evade detection. Constant evolution maintains the malware's stealth and allows it to exploit system vulnerabilities faster than signature-based defenses. Because these defenses rely on pre-identified th eat signatures, they struggle to keep up with the rapidly changing nature of adaptive malware.

As payments have moved beyond the simplistic four-party model, new participants—especially smaller ones who are less invested in cybersecurity—become the weakest link in the chain. These participants are often exploited by fraudsters as an entry point, compromising the resilience of the entire ecosystem.

Key traits

Polymorphism
Changes its structure (e.g., file signatu es) to avoid signature-based antivirus

Environment awareness
Adapts to the target system's defenses, like modifying execution paths to bypass fi ewalls

Autonomous decision-making
Uses machine learning to prioritize high-value targets or optimize infection speed

Key defenses

AI-enhanced endpoint detection and response (EDR)
Deploy EDR with real-time monitoring and automatic isolation of suspicious processes

Behavioral analysis
Monitor for unusual system activity (e.g., unexpected file changes, network spikes, etc.) and integrate user and entity behavior analytics to identity anomalous activity

Zero-trust architecture
Enforce strict access controls and multi-factor authentication (MFA), assuming no process or user is safe

Threat intelligence and patching
Remain updated on malware trends and automate patch management to plug vulnerabilities promptly

TREND #3

Ransomware attacks targeting payment systems

Ransomware attacks are evolving, increasingly targeting the payments ecosystem to hack critical technologies and steal data, necessitating robust cybersecurity defenses.

Cybercriminals are using malware programs to hack and commandeer business-critical technologies—such as customer databases, financial systems, and supply chain management software—then they demand a ransom, often large sums of money, in exchange for relinquishing operative control.

While ransomware risk permeates all industries, cybercriminals are increasingly directing their attacks at the payments ecosystem. For example, in addition to or instead of disabling core systems, the perpetrator may also steal private account data. And, unless ransom demands are met, cybercriminals may threaten to publish this data online or sell it to the highest bidder.

Ransomware-as-a-Service (RaaS) has emerged as a significant threat in the cybersecurity landscape. This business model allows cybercriminals to offer ransomware software to other criminals or affiliates, who then carry out attacks. In return, the original providers receive a share of the profits.

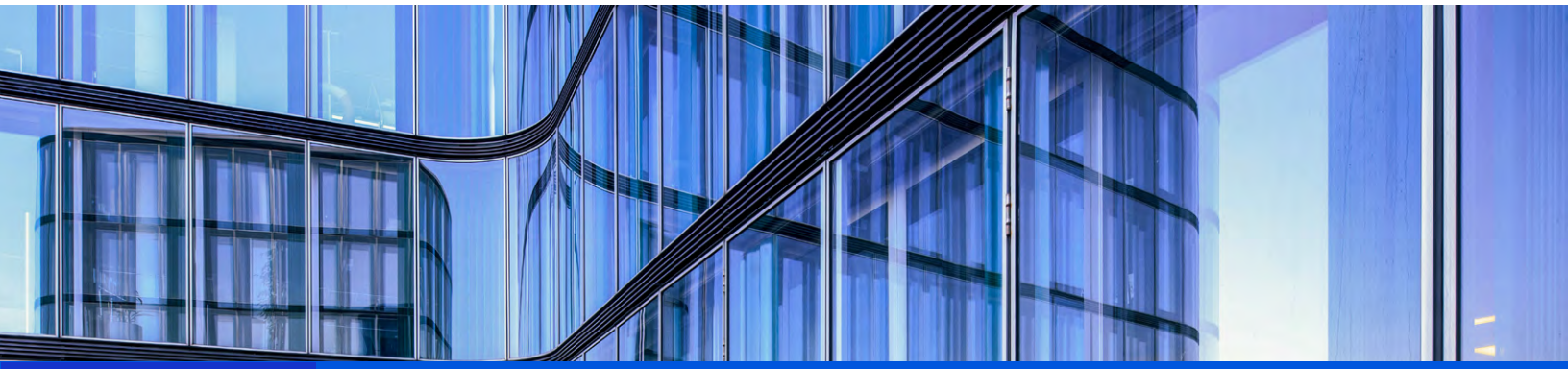
To prevent such attacks, companies can offer or mandate employee training around responsible data use and detecting and reporting cybercrime attacks (e.g., smishing, email phishing). Companies can also apply a rigorous approach to cybersecurity by reducing their attack surface, applying robust security protections, and complying with industry standards.

Even the smallest participants should adopt a foundational cybersecurity framework that includes the following elements:

- Define a cyber-risk appetite in line with regulatory requirements and business tolerance
- Develop a predefined incident response plan for detection, management, and recovery
- Implement data classification, encryption, and devaluation (similar to tokenization but beyond just PANs)
- Utilize DevSecOps practices, including automated code scanning to continuously search for worms and malicious code inserts
- Conduct regular Red Team/Blue Team simulations to test and improve resilience

By incorporating these measures, businesses can better protect themselves against cyber threats and enhance their overall security posture.

Additionally, companies can adopt a “defense-in-depth approach”—one that includes detective and preventive controls to prevent threat actors from gaining access to the network and deploying ransomware. If preventative measures fail to prevent the attack, it is crucial to have robust recovery safeguards to help ensure operations are swiftly restored from secure backups to minimize productivity loss.



TREND #4

AI-powered social engineering attacks

Social engineering, the psychological manipulation of individuals to divulge confidential information or perform actions that compromise security, has evolved dramatically with the integration of artificial intelligence. This concerning trend represents one of the most significant emerging threats in cybersecurity today.

Online social-media sites and networks are now so pervasive in today's digital world, many users see their online communities and identities as extensions of their real ones. As such, users may share sensitive personal information to develop online relationships and create new connections. Social media sites host massive amounts of user-provided data and are thus rich targets for hackers, particularly those using social-engineering.

Social media users commonly disclose personal identifying information, such as workplace details, travel plans, and relationship statuses. This can be exploited by cybercriminals, especially with applications like Geospy that can pinpoint the location where a photo was taken. Such tools provide unprecedented access to data, enabling highly targeted attacks.

Unlike traditional phishing attempts marked by glaring grammatical errors, odd messaging, or overly generic approaches, modern AI-crafted messages are more convincing, generated to reflect an individual's speaking and writing style, relevant personal details, and reasonable human-like conversation.

Preventing social engineering attacks

- **Verify requests independently**
  Confirm any unusual requests through official channels, especially those involving sensitive information like financial data
- **Be skeptical of urgency**
  Social engineers often create artificial time pressure; taking a moment to verify before acting on urgent requests is advisable
- **Use multi-factor authentication**
  Implement MFA on all accounts to add an extra layer of security beyond passwords
- **Limit personal information online**
  Regularly audit social media privacy settings and consider what personal details are shared publicly
- **Question unexpected communications**
  Be wary of unsolicited messages, even if they appear to come from trusted sources
- **Keep software updated**
  Ensure all devices have current security patches and antivirus protection
- **Educate employees**
  Regular security awareness training helps individuals stay informed about common social engineering tactics and emerging threats

TREND #5

E-skimming attacks on payment accounts

The payments landscape operates in an ecosystem that relies on the use of account details.

Account numbers, CVV2 and expiration date are constantly under intense scrutiny from cybercriminals, who are probing for new ways to obtain fresh details, and an emerging threat is the rise of e-skimming or digital skimming.

Attacks involve the injection of malicious code into a merchant's e-commerce systems to harvest payment card details as they are entered during checkout. If successful, hackers can often maintain access to the compromised servers and move around within the merchant's wider network.

To combat attacks, the onus of responsibility generally falls on merchants and their vendors to ensure updated cybersecurity protocols are effectively deployed. Consistent governance will help ensure that protective software is always updated and patched, robust firewalls are in place, permissions to access administrative portals are monitored, and systems are regularly audited for vulnerabilities or malware. Additionally, techniques such as tokenization, which replaces sensitive account data with a unique identifier or token that cannot be used if intercepted, are increasingly used to desensitize account data.

Two responses for organizations to consider

Partner your cybersecurity and payment fraud organizations

High-performing organizations that excel in risk mitigation hold a holistic view of cybercrime, financial fraud, and payments risk.

These organizations recognize that their adversaries have a sophisticated knowledge of the payment ecosystem and the role of payments businesses within it. They understand that cybercriminals are aware of the types of processes, controls, and vulnerabilities that arise from siloed organizations and governance. Additionally, they recognize that the biggest threats tend to reside at the intersections, as do the most effective solutions.

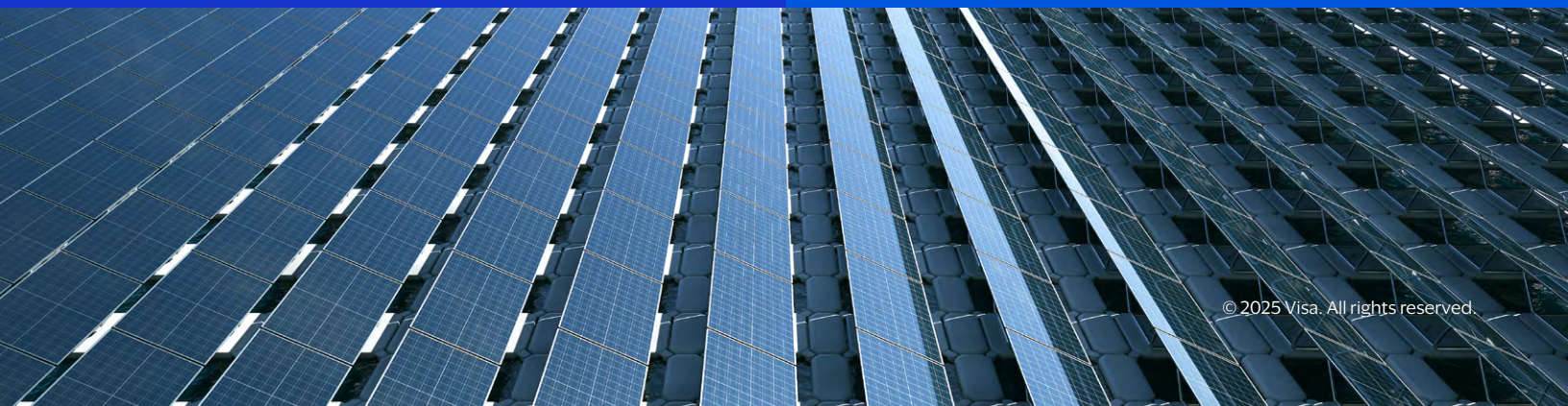
As a result, these organizations have structured their teams and processes accordingly. They combine risk management expertise (traditionally associated with fraud management teams) with technology expertise (traditionally associated with cybersecurity teams). Going beyond collaboration, they strive for true co-location and active collaboration.

Create a cybersecurity strategy framework using key security principles

Leading risk teams, comprised of cybersecurity experts within top-performing organizations, have established global security principles around identity and access management, cryptography and infrastructure, and application security, and have developed a comprehensive cybersecurity strategy.

These teams set the benchmark for best practices in cybersecurity, providing a model for others to follow in mitigating risks and protecting sensitive information.

Their framework—design, define, diagnose, defend—is considered a strategic imperative. As such, they collaborate across lines of business, including technology and data teams. They also secure executive leadership buy-in from the start to ensure sponsorship and funding.



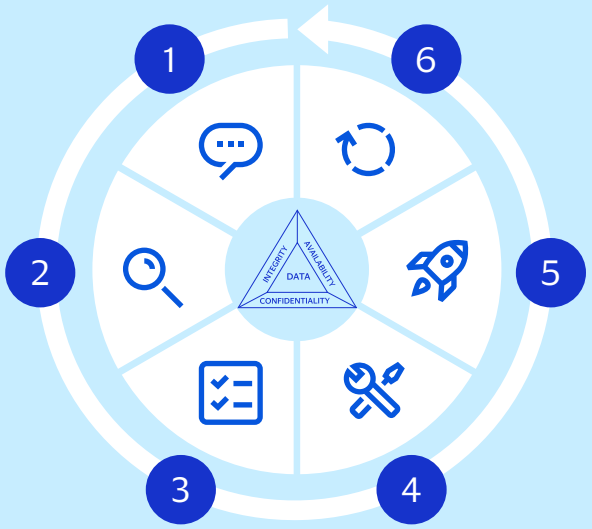
How Visa can help

Visa utilizes VCA's global network of consultants, data scientists, and product experts to help clients navigate the cybersecurity landscape.

VCA is ideally positioned to work with clients to help formulate a cybersecurity strategy, risk governance and compliance assessment and provide cyber training, awareness and education. Similarly, subject matter experts (SMEs) can assist in areas such as operational resilience including vulnerability management and patching, identity and access management, application security and ethical hacking, data protection and incident response readiness assessments.

VCA Advisory Services

Our six-step methodology provides a thorough assessment of your business and its cyber threats, implementing strategic enhancements and establishing a resilient recovery plan.



Awareness
Spread global trends and create a cybersecurity culture.

Identify
The key elements to review and manage cybersecurity risk.

Evaluate
Assess cybersecurity levels to create corrections plans.

Improve & detect
Make changes and improvements to detect cybersecurity vulnerabilities and threats

Execute
Build measures to counteract and neutralize cybersecurity incidents.

Recover
Recovery plans to restore services based on the nature & severity of the incident.

VCA offers a comprehensive range of services to guide clients in formulating a robust cybersecurity strategy. These services include:

Payment Cybersecurity Institute
Training and awareness programs for employees about payments cybersecurity best practices

Cybersecurity maturity assessments
Evaluate process and journeys to provide recommendations for improvements

Vulnerabilities Test / Assessment
Pentest to detect vulnerabilities on apps that could be exploited by hackers.

Threat Intelligence
Identify threats on the dark web threat and prevent attacks.

Enumeration Defense
Prevent from enumeration attacks with dedicated support.

About Visa Consulting & Analytics

- Our consultants are experts in strategy, product, portfolio management, risk & cybersecurity, digital and more with decades of experience in the payments industry.
- Our data scientists are experts in statistics, advanced analytics and machine learning with exclusive access to insights from VisaNet, one of the largest payment networks in the world.
- Our economists understand economic conditions impacting consumer spending and provide unique and timely insights into global spending trends.

We are a global team of thousands of payments consultants, data scientists and economists across six continents.

The combination of our deep payments consulting expertise, our economic intelligence and our breadth of data allows us to identify actionable insights and recommendations that drive better business decisions.

About Visa Risk

Securing the payments ecosystem requires continuous investment and innovation in new technology and collaboration with our business partners. Our job is to protect and enable Visa and its ecosystem partners to be the most secure, resilient, and trusted engine of commerce for everyone, everywhere.

We advance global and local market security initiatives by actively sharing intelligence and best practices, discussing evolving security trends and promoting collaboration on interregional and global risk issues.

Visa Risk also leverages a suite of network-level capabilities, analytics and expertise to protect the safety and soundness of the payments ecosystem and minimize fraud losses for its clients.

To get started, reach out to your Account Executive directly. Learn more about the team, resources, and our data-backed insights on Visa.com/VCA, and follow the team on LinkedIn.