Selecting the right cybercrime-prevention solution

Key considerations and best practices for achieving effective, sustainable cybercrime prevention

Introduction

Financial institutions, commercial enterprises and government organizations are all prime targets for cybercrime. Malicious software, or malware, is the primary attack tool used by cybercriminals to execute account takeover attacks, steal credentials and personal information, and initiate fraudulent transactions. The attack tactics, or crime logic, are constantly becoming more sophisticated so they can continue to exploit human and system weaknesses. Fraud-, risk- and IT-security professionals are looking to establish an effective defense against these attacks.

IBM Security Trusteer solutions have been helping to protect users against cybercrime since 2006. Based on our accumulated experience with hundreds of customers, thousands of fraud cases and millions of protected endpoints, we have identified the key principles and best practices for selecting cybercrime-prevention solutions.

This white paper discusses key considerations and best practices to help organizations achieve effective and sustainable cybercrime prevention.
Selecting the right cybercrime-prevention solution

Key requirements for effective, sustainable cybercrime prevention

When looking at deploying a cybercrime-prevention solution, organizations must consider multiple requirements. Beyond the core requirement of providing effective fraud prevention, the solution must address deployment costs, management complexity, impact to customers and regulatory compliance. This white paper will examine some of these requirements and will compare and contrast various approaches to addressing them.

• **Near real-time threat intelligence and visibility**—Malware can bypass virtually all security controls. An effective cybercrime-prevention solution must be able to assess changes in the threat landscape. This is essential to maintaining an effective defense that can protect customers over time.

• **Rapid protection against evolving threats**—Because all types of security controls are eventually attacked by malware, these controls must be able to adapt and stop new attack vectors. This is a particular concern with hardware-based solutions, or solutions that rely on statistical approaches to detect fraud. Often, it is extremely costly and complex for these types of solutions to respond to new attacks that attempt to bypass them.

• **Layered security**—Using multiple layers of security on endpoints and web applications makes it possible to achieve powerful and flexible protection. Endpoint security provides prevention, intelligence and remediation capabilities, and web-based malware detection provides instant coverage and lower deployment impact.

• **Early malware detection**—Malware is the root cause of most fraud. Preventing malware from infecting endpoints and attacking browsers or web applications can help prevent fraud from occurring. This requires complete protection of users' online activities, beyond online banking. Early prevention can also reduce the number of false positives and negatives handled by fraud and support teams that often result in higher operational costs and staffing requirements.

• **Limited impact to end users**—To help ensure that users adopt fraud-prevention measures, the impact on their day-to-day workflows must be significantly reduced without compromising protection. Solutions such as virtual browsers and hardware tokens sacrifice usability for perceived better security.

• **Cost-effective deployment, management and operations**—Fraud-prevention solutions should deploy quickly and require limited intervention from fraud, risk and support organizations.

• **Reliable cybercrime-prevention partner**—Ultimately, fighting cybercrime is a team effort. Any technology partner you choose must augment your staff with the expertise and capabilities to help you sustain an effective defense against cybercriminals.
Near real-time threat intelligence and visibility
As noted in the current Federal Financial Institutions Examination Council (FFIEC) guidance, the effectiveness of security measures used by financial institutions has eroded since the FFIEC issued its previous guidance in 2005. This realization has prompted the FFIEC to require financial institutions to conduct continuous risk assessments and adapt their security controls to address changes in the threat landscape.

Risk assessment represents a considerable challenge to many organizations. Fraud and security teams must gather threat intelligence from various sources, understand the threats that target their region, industry and specific institution, and determine if their controls are adequately addressing these threats. Performing threat analysis requires technology and expertise that are not available to many financial institutions.

Some cybercrime-prevention solutions attempt to isolate the user from malware as they access sensitive web applications by using virtualization technologies contained in hardware devices or available as software downloads. However, no security control can eliminate the need to perform risk assessment. Plus, lack of threat intelligence delays the response to malware attacks until fraud incidents start to mount. This can be detrimental to a financial institution’s bottom line, brand and customer retention rate.

Bottom line: If a financial institution cannot conduct its own threat research, it should partner with an organization that has the processes, people and expertise to gather and analyze threat intelligence and perform continuous risk assessment. Threat intelligence must be converted into specific actions in a timely manner to help ensure security controls remain effective.

Adaptive protection against evolving threats
The mirror requirement of threat intelligence is adaptive protection. Once a new threat or a new attack vector is identified through the risk-assessment process, a countermeasure must be rapidly developed and deployed across all protected applications and users. Financial institutions should assume that even their latest and greatest security controls will eventually be attacked by malware, and they must be able to respond immediately when this happens.

Bottom line: Adaptive protection entails a timely, automated and scalable process to update security controls against emerging threats. The update process should be transparent to end users and require limited involvement from the financial institution’s IT and fraud teams.

Layered security
Layered security is a fundamental best practice in cybercrime prevention. Endpoint controls form the first layer that secures end user devices against malware infection and attacks on client applications such as the web browser. Web-based controls create a second layer that detects high-risk users, devices and sessions. Combined, these two layers provide a formidable barrier to cybercrime using different techniques during different parts of the transaction lifecycle to help prevent and detect fraudulent activity.
**Bottom line:** Financial institutions should consider the solution’s overall cybercrime-prevention architecture. Through phased deployment of multiple protection layers that are centrally controlled and managed, it is possible to optimize security without increasing complexity and costs.

**Early malware detection**
Since the root cause of most fraud losses is malware, preventing malware from infecting customer machines and tampering with transactions is critical to helping prevent fraud.

Preventing malware infection requires protection of the user’s overall online activity. Users can become infected when visiting any website, and phishing attacks can happen outside the context of an online banking session. It is therefore essential to secure all online activities on the end user machine beyond the specific online banking site.

Certain approaches to fraud prevention focus on identifying fraudulent transactions. Fraud detection occurs when a fraudulent transaction is submitted but before funds are withdrawn from the account. Due to the statistical nature of these approaches, a false positive or false negative is likely to occur. With false positives, the fraud team must review many legitimate transactions, which is a costly and resource-intensive process. With false negatives, a direct cost of fraud loss is virtually guaranteed and subsequent indirect costs, such as brand damage and customer turnover, soon follow. Cybercriminals also take many steps to help ensure that fraudulent transactions “fly under the radar” by exhibiting as many characteristics of normal, customer-generated transactions as possible.

Other approaches focus on isolating the online banking session from malware. History has shown that once a host is infected with malware, it is possible to attack any security control that executes on the infected machine. Virtualization-based browser solutions are no exception, and these are susceptible to memory injections into their processes executing on the underlying host.

Conversely, strong endpoint security controls can help prevent an initial infection, which is the first step in the attack lifecycle. If malware already resides on the machine, it can be stopped from attacking the browser and other key services, a vital component of setting up the attack. A clientless malware-detection layer can directly identify infected, high-risk users before an actual fraud attempt occurs, and feed risk data into risk engines. An adjusted transaction risk score can be used to restrict access to functions such as adding a payee or transferring money. In both cases, endpoint-centric security controls can help directly detect and protect against malware on the endpoint—not just its side effects.

**Bottom line:** Effectively containing fraud losses favors stopping malware from ever generating a fraudulent transaction. Look for a solution that uses malware prevention and detection layers as cornerstones of security control, as this can help significantly reduce the number of suspicious transactions that fraud teams have to deal with—and the likelihood of fraud losses.
**Limited impact to end users**

Cybercrime prevention is a balancing act of security, transparency, usability and interoperability. Server-side solutions offer transparency but also reduce fraud-prevention capabilities, as they often lack visibility into endpoint malware, the root cause of most fraud. Some endpoint solutions require end users to change the way they access web applications to reduce exposure. The impact of these solutions on end user acceptance and adoption of fraud prevention solutions can be substantial.

Typically, end users prefer to continue using their devices and commercial browsers of choice, as well as to be able to print and use third-party applications. Furthermore, financial institutions should aim to provide protection in the background with limited user interaction.

**Bottom line:** To encourage end users to adopt fraud-prevention solutions, financial institutions should choose an option that limits the impact to their users’ day-to-day workflows. If users’ well-being is ignored in the name of better security, users might hesitate to employ the proposed security controls—which can seriously compromise security efforts.

**Cost-effective deployment, management and operations**

While fraud-prevention products should be simple to deploy and operate, actual implementation costs and complexity levels vary dramatically among different products.

During initial deployment, some solutions require substantial effort to establish and sustain a statistical baseline for normal user activity. Once the baseline is established, fraud teams must pursue a large number of possible fraud cases that are based on deviations from the profile, many of which are false positives. Ultimately, when fraud losses occur or fraudulent transactions are detected, financial institutions face very limited options for remediation, as removing malware is a complex and daunting task.

Other approaches require distribution of hardware devices or complex software to end users. These deployments incur shipping, tracking and provisioning costs, cumbersome and complex update processes, and logistics overhead when devices have to be replaced if lost or malfunctioning.

Consider the following characteristics of a cybercrime-prevention solution that is simple to deploy and operate:

- **No changes in user workflow and environment**—Users prefer not to use awkward devices that can be stolen or forgotten, or to change the way they use online banking. The solution should support their browser of choice (Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari), their PC platform (Microsoft Windows and Mac) and third-party applications that support business processes.

- **No false positives**—Accurate fraud detection is a core requirement of cybercrime prevention. Financial institutions should not expect a plethora of alerts and warnings to be investigated. The more visibility the solution has to the threat landscape, the more accurate it will be in detecting malware-driven fraud.

- **Scalable to all channels (retail and business)**—Financial institutions need to protect all channels with hundreds to millions of users. Patching together multiple technologies that claim security without scalability creates redundancies and management overhead.

- **Remediation and malware removal**—End users and financial institution support teams face the task of restoring endpoints to a clean state following a malware-driven fraud attempt. Often, end users have no choice but to reformat their computer hard drives or restore the operating system to its factory settings. Both approaches are highly disruptive. A cybercrime-prevention solution should go beyond detection and prevention to offer an automated way of removing malware without the need for complex and disruptive procedures.
• **No hardware or software to install at the financial institution**—IT organizations are increasingly adopting Software-as-a-Service (SaaS) solutions that can reduce the burden of deploying and maintaining enterprise software applications. In the case of cybercrime-prevention software, SaaS allows the solution provider to leverage threat intelligence across multiple customers and to rapidly update its protection capabilities, creating a strong network effect.

**Bottom line:** Cybercrime-prevention solutions should allow for quick deployments and significantly reduce the rollout and support requirements from financial institutions and end users. Malware removal and remediation capabilities should enable infected users to quickly restore their systems to a clean state, so their productivity is not affected.

---

**Reliable cybercrime-prevention partner**

Cybercrime prevention is a process. A financial institution’s trusted cybercrime-prevention partner must be able to continuously monitor the threat landscape, gather intelligence and adapt its security controls against emerging threats. The key ingredient of this process, *intelligence*, is derived from the vendor’s marketplace presence. Simply put, technology is not enough. The vendor must have the global customer footprint and operational track record to demonstrate that it can effectively detect changes in the threat landscape, analyze them and sustain the effectiveness of its security controls over time.

**Bottom line:** A reliable cybercrime-prevention partner has a broad global presence, an established customer footprint and a demonstrated ability to deliver sustainable fraud prevention over long periods of time.

---

**Figure 1: Four principles of successful fraud-prevention architecture**

- **Fast time to value**
  - Light integration
  - Unified platform: any scale

- **Effective and accurate**
  - Focus on the root cause
  - Prevent first, detect next, early

- **Seamless experience**
  - Transparent to customers
  - Significantly reduce “busy work” to staff

- **Adaptive controls**
  - Near real-time intelligence
  - Dynamic software vs. static hardware
Conclusion
When selecting a cybercrime-prevention solution, it is imperative to realize that, over time, no static security control can remain effective at stopping malware-driven online banking fraud. Sustainable cybercrime prevention can be achieved only by coupling layered adaptive security and near real-time threat intelligence delivered by a reliable cybercrime-prevention solution partner. Furthermore, financial institutions must consider the ability of solutions to leverage security controls quickly and cost efficiently, without being hindered by poor usability, limited platform support, long deployment processes or late detection of fraudulent transactions.

Why IBM?
IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The proven technologies enable organizations to protect their customers, employees and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information
To learn more about IBM Security Trusteer cybercrime-prevention solutions, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

About IBM Security solutions
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM® X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing