Kriptone

Independent Contractors in the Banking Industry.

Trust, but verify

Hiring third-party contractors became an essential part of the business strategy in many industries. While working with remote vendors is an essential part of corporate workflow, a major security issue arises. As independent contractors often share the privilege of accessing your network with regular employees, how can you protect your network from exposing and leaking sensitive data?

This problem became a hot issue throughout the IT industry, especially for the financial sector and data centers as information is considered to be their most guarded asset. This whitepaper examines the issue of monitoring third party vendors in the banking and financial sector, and suggests possible solutions.

Who is an “independent contractor” exactly?

Independent contractors are organizations or individuals hired by a company to provide services, who are not the company’s full-time employees. Independent contractors are often referred as **third-party providers, remote vendors, freelancers, trades or consultants**. Many employment protection laws and tax regulations covering full-time employment are not applicable to independent contractors, which often enables businesses to save time, money and effort by offloading parts of their operation to third parties.

What are the benefits of dealing with independent contractors?

Hiring a remote contractor to do a one-time job is plain cheaper and faster than opening and filling a position. Dealing with independent contractors is easier on the accounting, too. A long-term relationship with a specialized data management, marketing or IT security provider brings even greater benefits compared to in-house solutions. At the same time, many jurisdictions impose legislations to limit the use of independent contractors on permanent basis in lieu of full-time employment.

The **higher flexibility, the cost savings, the ease of accounting** and the ability **to fill the position quickly** often become deciding factors when hiring a freelancer. This is especially true if the company needs a contractor to handle a specific, time-limited task, without having to open a new position and grow its own specialists dedicated to performing **non-core tasks**. The expertise, reputation and professionalism of specialized service providers can help banks quickly solve problems they would otherwise spend months and years to address. In other words, independent contractors and service providers are not going away any time soon.

The “ifs” and “buts”

Despite the advantages, many banks are wary of hiring independent contractors specifically because of security issues and corresponding legal concerns. Banks are rightfully concerned about the risks of exposing sensitive data, their customers’ financial information or IT infrastructure to third parties.

Today, the term “third-party contractor” has gone beyond the traditional meaning of goods and service providers to include contractors dealing with the bank’s data infrastructure across the banking ecosystem. In the banking supply chain, data is a very important asset that must be protected, and only managed, handled and stored according to corporate, regulatory and legal rules.

Third-party vendor management is also important from the compliance standpoint. **Security is only as strong as its weakest link.** A single exposure resulting from a weak process or policy could render the entire security infrastructure inefficient.

Symantec and Prevalent recently hosted an expert online panel on cybersecurity and third-party risks. Here are the highlights from this session:

- Businesses have very little visibility into the information that is being shared, with whom the information is being shared, and the security practices and protocols of third and fourth parties that have access to the information.
- Businesses also have very little visibility into the provenance of the data that is entering its networks.
- Malicious hackers and data grabbers are increasingly targeting the less secure, smaller third and fourth party partners or a business' regional or field units as backdoors to the parent organization's data centers.

Can you trust your remote vendors?

Managing third-party contractors is critical for securing sensitive business data and customer financial information. A remote contractor or supplier can provoke a data breach. Most terrifying is the thought that the bank itself may **never know about the incident**, and even if the leak were discovered, it could never find out the **real cause of that accident**. Sometimes it is only possible to discover the truth if your contract requires the vendor to notify you about all security events.

In the past two years, the following large contractors have experienced a data breach: Adobe, LexisNexis, Dunn & Bradstreet, Kroll Background America (HireRight), J.P. Morgan, State Farm, Kaiser Permanente, and Epsilon. What if one of them was on your vendor list?

Each bank relies on securing its confidential data and complying with legal regulations. That is why it's important to make sure that suppliers and contractors handle information assets securely and with the level of care you require.

Regulatory compliance

Managing remote vendor has never been easy for banks due to **regulatory compliance issues**. Regulations are constantly changing, and banks must implement constant changes to comply. Would you rather have the vendor working for your bank, or your bank working for the vendor?

Effective vendor management can provide additional value far beyond reducing risk and satisfying regulatory requirements. Vendor management can increase net profits, improve contract terms, reduce costs from audits, and encourage better performance from contractors.

Controlling the risks associated with remote vendors: looking for a solution

The easiest way to eliminate the risks connected with third-party contractors is not hiring third-party contractors. This, however, is not an option for many organizations.

Thus, banks need to build a stronger **vendor security**. Banks have been using third parties to achieve strategic goals for years. According to existing legislative policies, market and economic conditions, banks need to pay close attention to managing independent contractors.

While many reliable third-party contractors exist, they are not governed by the same high standards and regulations as the banking industry. Contracting a third party becomes a difficult mission and a known risk in the era of information technologies. To control the risks, one must control the contractor.

A well-written contract outlining the duties, obligations and responsibilities of the parties is a necessary requirement, but not nearly enough to ensure compliance.

Sometimes, hiring yet another independent contractor (such as a specialized security company) to watch remote contractors may be tempting. However, this can quickly become a vicious circle, introducing yet another weak link into the security chain.

Numerous methods exist to control independent contractors. However, **installing a proper monitoring system** goes a long way helping the bank auditing remote vendors and suppliers while using in-house resources.

Unfortunately, only a counted few products will fit the job. Moreover, most of them are not directly intended to monitor third party suppliers.

Existing solutions: video surveillance or computer monitoring?

Traditionally, organizations were relying upon video surveillance to control employee activities. Unfortunately, traditional surveillance cameras don't capture the required level of detail, and are completely unable to monitor remote and terminal sessions.

Software-based monitoring solutions exist, enabling employee monitoring over corporate networks. Some of them are suitable for monitoring remote contractors. But only a few solutions

have both server and workstation agents. In addition, many of these solutions are not exactly easy to use, generating a set of logs files for various aspects of system use and data access operations. Most are quite resource-intensive, time-consuming to analyze and requiring significant financial investments.

Capturing an indexed video stream

While neither video surveillance nor software log-based solutions are a perfect match for monitoring remote contractors, combining both approaches into an innovative video-based surveillance system does the trick.

Instead of recording on-screen activities with a dedicated surveillance camera, the new approach aims to records remote sessions and on-screen activities with screen capturing software, saving successive screen shots into a **chaptered and indexed video file**. Captured video streams are easy to navigate thanks to accompanying text metadata including the name of the active application, currently opened Web URL, mouse activities and any keyboard input entered by the local or remote user including logins and passwords.

All this combined creates a perfect system allowing to audit everything taking place on the computer screens within the organization. This new approach gains momentum in the area of workstation monitoring. But what about servers?

Monitoring privileged users

While some remote contractors enter the network as **ordinary users with restricted access and low privilege level**, some jobs require the use of **administrative access and elevated privileges**. As a result, some third-party vendors will have privileged access to enterprise servers. This can easily become your weak chain. Thus, terminal session monitoring is an essential part of the enterprise security chain. Monitoring privileged user access is an essential part of every company's security infrastructure.

Recording all activities performed by regular and privileged users during a terminal session delivers the required level of security and helps mitigate risks imposed by a third party accessing your network. A video capturing system provides **fully indexed and complete searchable video records** of all actions performed on your servers. Reviewing and analyzing these video records does not require any specific technical skills other than those possessed by a qualified security officer.

Take a look at the Ekran System solution

Existing solutions corresponding to the high requirements listed above are quite expensive. This is why we created a solution of our own. Ekran System combines all the powerful features required to secure a bank's corporate network while offering immediate cost savings compared to competition.

Ekran System is a modern solution for your corporate network to enable monitoring and auditing of independent service providers. This innovative computer surveillance system is based on capturing on-screen user activities of regular and privileged users, and creating a fully indexed and easily searchable video stream. Ekran System can monitor all workstations and servers in the corporate network including local, remote and terminal sessions. Installed on a server or workstation, Ekran Client records a video stream of all sessions belonging to regular and privileged computer users, and captures accompanying metadata such as the current application name, window title, URL, keystrokes, and so on. This metadata is tied closely to the video stream, enabling full-text search through the recorded video.

Ekran enables easy playback for all recorded sessions. Coupled with full-text search, the system enables administrators to quickly find key episodes to investigate incidents and analyze productivity and compliance of internal and remote employees, administrators, or third-party service providers.

Thanks to the easily accessible video records, administrators will be able to discover all instances of internal data misuse, competitor contacts, issues of fraud and theft of intellectual property.

Don't take chances with PCI DSS, ISO/IEC 27001, ISO 27011, APP, EU DPD 95/46/EC compliance. Try Ekran System now to manage remote vendors, mitigate the risks of non-compliance, and reduce costs. For more information visit www.kriptone.com