blue umbrella

Guide | Best Practices for Compliance

Gaining the High Ground

IT Security Third-Party Risk Management

Cybersecurity Behind and Beyond the Firewall

- Employee Processes
- Data Access Controls
- Data Center Access Controls
- Data Privacy and Retention

Dollars to donuts, every aspect of your business is accelerating. Everyone is now capable of accomplishing almost any task at greater velocity, with potentially greater impact. Unfortunately, this truth also extends to dangerous oversights and nefarious deeds. Criminals want your corporate data, and if you're not on top of IT security every millisecond of every day, it can all unravel at the speed of light.

At the same time, regulations like the European Union's General Data Protection Regulation (GDPR) and the new California Consumer Privacy Act (CCPA) demand exceptional levels of oversight and governance for your data infrastructure. If cybercriminals don't catch any slip-ups, regulators just might.

Third-party management is the processes a company uses to monitor and manage interactions with all external parties with which it has a relationship.

Either way, everyone needs to be on their game. But as hard as it is to lock down your own organization, how do you ensure all the businesses in your supply chain go to similar tlengths to prevent data leakages?

Third-party IT Security Matters

Growth remains the top strategic priority for CEOs of medium and large-sized companies in 2019-2020, according to Gartner's 2019 CEO and Senior Executive Survey.

Achieving growth in today's market often requires strategic partnerships. As your business relationships expand with vendors, partners and agents, your risk exposure grows exponentially. Any data connections between your enterprise network and that of third-parties means vital information could be shared or access compromised.

75% of Fortune Global 500 companies will treat third-party risk management as a board-level initiative

— Gartner

In the digital space, just like the real-world supply chain, you're only strongest as your weakest link. It's a universal concern for IT Security professionals and compliance officers.

This concise guide will help ease your mind. It offers best practices for your organization to consider as part of its compliance risk management policies and procedures, including the most common third-party threats to monitor, offboarding practices you should require, and how to move quickly to identify and remediate any issues.

Cybersecurity behind and beyond the firewall

IT security practices have to adapt to fast-changing threats. In an ultra-connected, automated digital world, it is easier than ever to gain access to data and technology systems, or crash them.

At one time, Distributed Denial of Service (DDoS) attacks would simply flood a target's servers with false requests to connect, attempting to consume enough server resources to make the system unresponsive to legitimate traffic. Now, DDoS attacks are more intricate (as well as more frequent and more powerful), targeting services, infrastructure and software.

Multi-vector attacks are more common, too, in which hackers using two or more methods of network infiltration —out of dozens of possible vulnerabilities—at the same time. Some of the most common: email, social media, databases, web browsers, USB flash drives, mobile apps and even online ads.

Sophisticated multi-vector attacks used to require a high level of skill by the hacker. Now cybercrime has advanced to the point that it's possible for almost anyone to launch these attacks.

52% of data breaches were caused by external hacks
39% of breaches involved organized crime groups
33% of these exploited social media
28% involved malware

— **Verizon 2019 Data Breach Investigations Report**

And that's just the tip of the iceberg. So-called "Low and Slow" attacks extort money by stealth using crypto mining-based malware. Ransomware locks out users until Phishing tricks present themselves as trustworthy in order to trick people into providing sensitive information. Soon "smishing" (targeted attacks via SMS) and even "vishing" (targeted attacks through voice communication) may be a concern.

No Technology is Flawless

For third-party risk management, it's important to gather evidence that your vendors, partners and agents have policies and procedures in place to mitigate the growing spectrum of potential attacks or vulnerabilities—and if necessary, respond effectively. Specific technology can better protect some systems (secure email gateways, for example, can prevent phishing attempts with proxy and time-of-click analysis filtering), but no technology is flawless.

22% of organizations have limited resources available to respond to a security incident

— **2019 Incident Response Report**

According to a 2019 report by BAE Systems, two-thirds of all organizations experience between one and 25 breaches every month.

You need to assess the level of sophistication each of your business partners, vendors and agents has toward cybersecurity. A few broad areas to consider:

- Change management — Are security assessments performed every time significant updates are made to applications or systems?
- Software development — Do they perform code reviews prior to releasing updates into production?
- Business continuity — Is there a documented plan, and is it tested at least annually?
- Incident response — What formal processes are in place?

Your company's third-parties must demonstrate a commitment to cybersecurity preparedness.

Employee Processes

For organizations to adequately protect IT infrastructure, they must acknowledge that the greatest risk comes from human vulnerabilities, not technology.

External cyberattacks now routinely prey upon human error or naivety to click on the wrong link to launch malware of some variety, or trick them to provide sensitive information, as is the case with phishing.

Educate to Mitigate

Regular education and training is a must—not just for full-time employees of your third-parties, but also any contractors or their own third parties who may get access to internal systems or sensitive data. Do they know how to securely handle or transfer different types of data?

34% of breaches involved an internal actor

— **Verizon 2019 Data Breach Investigations Report**

In an era of nearly limitless wireless connectivity and digital mobility through smartphones, tablets, laptops, and other networked machines, it's incumbent on everyone to self-police. Bring Your Own Device access is addressed below, but how much do employees recognize the risks of their own behavior to unintentionally cause a security breach?

Offboarding

On the other hand, *intentional* breaches caused by a disgruntled or former employee cannot be overlooked either. Whether personnel leave on good terms or not, your third-parties need well-documented policies, procedures and guidelines to govern employment and termination. How quickly is access revoked? Is it always clear how much access an individual has, and to what systems? How do they return any company IT assets they have in their possession?

To prevent data leakage or prohibited access, third-parties must consistently take steps to inform employees of updated cybersecurity guidelines, and ensure they change the proverbial locks after an employee leaves.

Data Access Controls

Who gets access to what, and how? If you're exchanging data with a third-party, it's vital you understand who can see it and under what circumstances.

Clearly your third-parties should restrict access to client data and authorize it only as needed. But who decides, and under what criteria? Is access requested via IT service ticket? The role they have been

assigned in a system? Is their access ever logged or monitored? What about unauthorized access attempts, or account lockouts? A third party should have detailed control principles implemented to secure sensitive data.

> **58% of enterprises have suffered a breach due to vendor access**
> **64% of organizations suspect a breach due to employee access**
>
> — **BeyondTrust Privileged Access Threat Report 2019**

Granting access is only one consideration. What steps an individual must take to actually gain access is another matter.

Passwords are highly imperfect. To make hacking them harder, password control systems should require a certain level of complexity and frequent updates, and prohibit reuse. Ideally, multi-factor authentication should be in place, so logins require a code sent to a separate device.

Encryption

Exchanging sensitive data with your third-party must be done securely, even if it's over email. Transport Layer Security ("TLS"), for example, is one effective technology to support encryption or authentication of password-protected documents.

Multiple methods of data encryption are viable, for both data in transit and at rest. Cryptographic keys of varying degrees of strength can protect against unauthorized access or destruction of critical data. From a compliance perspective, they should meet or achieve the standards set by your industry regulations; from a practical IT security perspective, the specifics may be less critical than ensuring your third-parties do, in fact, support and properly manage encryption.

Devices on the move

Issues of encryption and access have become more important with the proliferation of devices. Long gone are the days of terminals secured within offices. Just like in heist movies, the security of an asset—even if it's digital data—is more vulnerable on the move.

Connecting over a wireless network, if access isn't properly restricted and encrypted, can expose data. Smartphones and laptops can go missing. Employees may use their own devices to access sensitive data.

Third parties can implement the right technology and policies to significantly reduce this IT security risk. They can start by putting in place formal "Bring Your Own Device" (BYOD) policy in place, maintaining a list of all approved mobile devices for storing and accessing company data. The truly committed will enforce, through technology controls, mobile device management and full-disk encryption on all laptops and other portable devices.

Data Center Access Controls

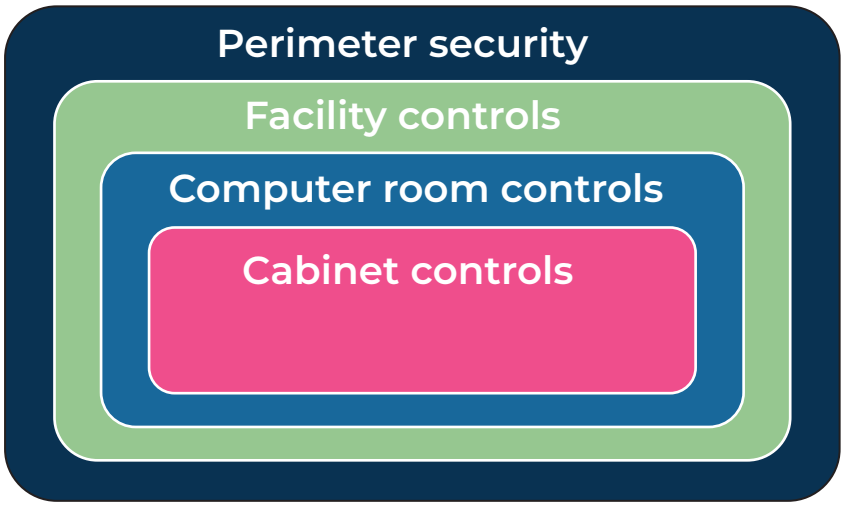
As much as mobile devices present significant IT security risks because they offer entry points to networks and data, most data ultimately resides physically inside a data center. Although the rise of cloud computing has abstracted this fact, and for many users it can feel like data exists somewhere out in cyberspace, in reality corporate information is stored on servers running in safe, encrypted data centers.

Your third-parties may or may not run their own data center, and they could even operate servers on premise at a corporate office. Regardless, they must have documentation of how those data centers are secured, in both a physical sense and the virtual protections in place for the networks and data.

Four Layers

There are four primary layers to data center security that need to be considered:

- Perimeter security
- Facility controls
- Computer room controls
- Cabinet controls



In some scenarios, your third party may not have four layers, but at each level, access needs to be managed and restricted. All visitors must have badges or tags that clearly identify employees, contractors and non-employees while on premise. If your third party operates servers inside its corporate offices, do not overlook this simple security measure.

All access should be logged, and identification verified. This could be through a unique password or PIN, an electronic pass assigned to the individual, or even biometric scans for fingerprints or irises. Who gets in and out of a facility that stores data has to be tracked, ideally as they pass in and out of each access level.

Data Privacy and Retention

Even with all of the other IT security measures noted above, you may still face third-party risk related to the data they store.

The GDPR and CCPA data privacy regulations require careful management of personal information—it should be kept accurate and up to date, and when it's no longer needed for business, it must be deleted.

From a compliance perspective, data retention is a growing issue that needs to be addressed by all companies. The challenge is even bigger when data is shared between partners, vendors or agents. If they have your client data, you need assurances that it will be handled properly.

Third-party organizations should demonstrate that they have policies and procedures in place to:

- Retain client data for only a limited time
- Return data to client once business is complete
- Securely dispose of media that contains its clients' data

As the world becomes more aware of the risks posed by personal information being misused or falling into the wrong hands, all organizations are under increased pressure to review what they do with collected data, and have a plan to document how they ultimately delete it. Ensure your third-parties are capable of complying with these practices while they have access to any client data—and just as importantly, for when your association together may come to an end.

Ready for Anything

Cybercrime has evolved into a highly sophisticated enterprise. It's easier than ever to launch all manner of attacks, and harder than ever to defend. As the world becomes increasingly powered by computerized data, the value of successfully breaching corporate IT systems only grows.

For third-party risk management, it's vital that your vendors, agents and partners show that they take IT security seriously. The number of "what ifs" organizations must consider is long, and will only get longer. Having an effective, comprehensive third-party IT security compliance program in place ensures that their level of preparedness is evaluated from every angle, and steps can be taken to close any gaps.

At the end of the day, working with third parties to improve a broad spectrum of cybersecurity best practices not only helps your business. It helps make our digital world safer.