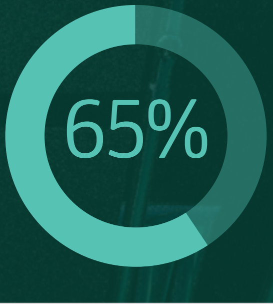
Five Best Practices to Manage and Control Third-Party Risk

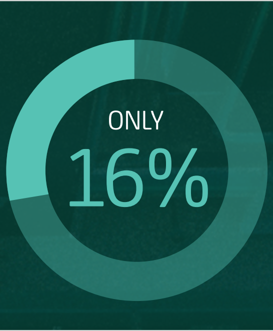
ca technologies

Data security risk caused by third parties is a pervasive problem.

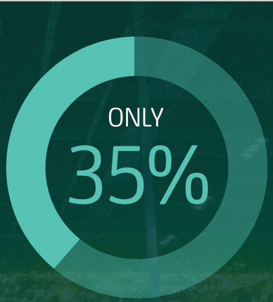
Yet, many organizations granting remote privileged access to third-party users leave gaps that represent significant security risks.



OF BREACHES CAN BE TRACED BACK TO A **THIRD PARTY**.[1]



OF ENTERPRISES **EVALUATE THIRD PARTIES' CYBER SECURITY** MORE THAN ONCE A YEAR.[2]



OF VENDOR RISK MANAGEMENT PROGRAMS IN THE FINANCIAL INDUSTRY WERE **FULLY MATURE** IN 2015.[3]

[1] Troy Leach, Chief Technology Officer of the PCI Council. [2] PwC. US Cybersecurity: Progress Stalled. July 2015
[3] Metric Stream. The 2015 Risk Management Association Third-Party/Vendor Risk Management Survey. 2015.

Have you done enough to protect your business?

If you're like most organizations today, you frequently grant vendors, contractors and other non-staff members access to internal networks and systems. These privileged users remotely administer your operating systems, databases or applications using their own endpoint devices.

The problem is, your security team may know little to nothing about these individuals or their companies' security practices. These users may be poorly vetted, third parties may have loose security policies and credentials may not be well protected. For these reasons, privileged third-party accounts often present the biggest risk to your enterprise.

In fact, reports of **cyberattacks now dominate the headlines**, and many—including the major breaches at Target, Home Depot, Goodwill and the U.S. Office of Personnel Management—were not caused by direct attacks on the companies themselves, but via breaches at third-party vendors. In most cases, attackers exploited stolen vendor credentials to gain unauthorized access to the ultimate victim's network and critical systems.

THE FALLOUT OF A DATA BREACH

$252 m

GROSS EXPENSES INCURRED BY **TARGET**[4]

$56 m

TOTAL NET LOSSES EXPERIENCED BY **HOME DEPOT**[5]

21.5 m

IDENTITIES EXPOSED AT THE **U.S. OFFICE** OF PERSONNEL MANAGEMENT[6]

868 k

PAYMENT CARDS COMPROMISED IN 330 GOODWILL STORES[7]

[4] The Conversation. Why Companies Have Little Incentive To Invest In Cybersecurity. March 2015.

[5] Ibid. [6] NBC News. OPM Hack: Government Finally Starts Notifying 21.5 Million Victims. October 2015.

[7] Forbes. 868,000 Payment Cards, 330 Stores Hit in Goodwill Credit Card Breach. September 2014.

Defend Against Privileged User Risks

If data breaches such as these have taught us anything, it's that assuming a partner will exercise good security practices is a recipe for disaster. But no modern organization can succeed in this digital age if they're isolated and disconnected.

To reap the benefits of a connected enterprise, sensitive information must be exchanged—and not just among employees, but with outside vendors, contractors and partners. However, restricting privileged accounts from unauthorized use isn't easy when the activities of the user occur outside the direct control of your information security team.

But with the right information security practices, you can help **protect your business from third-party risk** without closing off your enterprise or hindering legitimate business activities.

[3] *Assembling the DevOps Jigsaw*, Freeform Dynamics, 2015

5 Best Practices for Controlling Third-Party Vendor Risks

Many risks can be mitigated by using five best practices that work together to create a layered, strong, flexible and powerful information security defense. These practices include:

1

Implementing supporting processes and controls that define and enforce access policies for third-party privileged users.

2

Authenticating users better by using multi-factor authentication technology, so privileged credentials are harder to compromise, even in the face of social engineering and phishing attacks.

3

Separating authentication from access control, so privileged users have only limited visibility to internal networks, minimizing the possible damage one user—or one set of stolen credentials—can inflict.

4

Preventing unauthorized commands and mistakes with real-time policy enforcement as a first line of defense, protecting the infrastructure from malicious activity and mistakes.

5

Monitoring activity and investigating suspicious events to quickly catch breaches, improve training when needed and continuously refine automation and processes.

READ MORE

BEST PRACTICE 1:

Implement Supporting Processes and Controls

Business relationships can be established and system access may be provided without the knowledge or review of your information security team. So clear policies for defining, enabling and enforcing the access of non-employee privileged users must be a part of contract negotiations and vendor on-boarding procedures.

Define Policies | Assess Risk | Enforce Procedures

Start by establishing processes for training, provisioning, monitoring and de-provisioning third-party users. Be sure to clarify the systems and resources to which third-party users have access, along with the level of privileges needed to perform their duties.

BEST PRACTICE 1:

Implement Supporting Processes and Controls

Business relationships can be established and system access may be provided without the knowledge or review of your information security team. So clear policies for defining, enabling and enforcing the access of non-employee privileged users must be a part of contract negotiations and vendor on-boarding procedures.

Define Policies | Assess Risk | Enforce Procedures

According to Benjamin Lawsky, Superintendent of Financial Services for the State of New York, “a firm’s cybersecurity is often only as good as the cybersecurity of its vendors.” Just one partner with weak controls or poor security can provide hackers with a backdoor entrance to your data. So, from a risk management standpoint, the assessment of each partner’s security relative to your established organizational standards is a must. It’s also critical you ensure third-parties, just like your own organization, comply with mandates applicable to your industry, such as the PCI Data Security Standard and HIPAA HITECH.

BEST PRACTICE 1:

Implement Supporting Processes and Controls

Business relationships can be established and system access may be provided without the knowledge or review of your information security team. So clear policies for defining, enabling and enforcing the access of non-employee privileged users must be a part of contract negotiations and vendor on-boarding procedures.

Define Policies | Assess Risk | Enforce Procedures

Once assessment and processes are in place, they need to be enforced by the business units who own the vendor relationships and handle the associated operational processes, including onboarding and off boarding users and responding to reports of incidents.

Basic elements that need to be included in every third-party contract:

- **References** to the actual policies and procedures a vendor commits to enforce, including background checks and training of vendor employees with access to your organization’s systems.
- **Penalties** for non-compliance and remediation processes.
- **Checks and balances** available to validate compliance.

BEST PRACTICE 2:

Authenticate Users Better

It's not uncommon for a third-party to lack the security maturity of larger organizations, and this is especially true for credential management. Vendor and partner credentials are often too weak and are susceptible to inadvertent disclosure. The best way to protect credentials is to proactively manage and control them.

Apply Multi-factor Authentication | Eliminate Shared Accounts | Enforce Onboarding/Offboarding Processes and Procedures | Use Background Checks and Identity Proofing

According to recent statistics, the **success rate for repeated phishing attempts is close to 100%,** after just five to seven attempts. Once an organization is targeted, it's just a matter of time before credentials are compromised. The best way to prevent these stolen credentials from being exploited is by adding another factor into the authentication process. Several multi-factor authentication options are available, including certificates, hardware-based tokens, software-based tokens or verification processes that leverage a person's cellphone.

BEST PRACTICE 2:

Authenticate Users Better

It’s not uncommon for a third-party to lack the security maturity of larger organizations, and this is especially true for credential management. Vendor and partner credentials are often too weak and are susceptible to inadvertent disclosure. The best way to protect credentials is to proactively manage and control them.

Apply Multi-factor Authentication | Eliminate Shared Accounts | Enforce Onboarding/Offboarding Processes and Procedures | Use Background Checks and Identity Proofing

Eliminate Shared Accounts

It’s not uncommon for a third party to request a single account used by all employees to gain access to your systems. Though this approach is easier administratively, it presents a number of security headaches and vulnerabilities for your organization. For starters, multi-factor authentication and shared accounts don’t mix. Second, your ability to control access to and use of shared credentials is harder. Case in point: If a shared credential is used among multiple individuals, and one person leaves, that departing individual will continue to have access to systems unless the credential is changed. Third, it becomes impossible to determine which individual took a specific action on the network. Issuing credentials to individuals and not vendors helps eliminate these problems.

BEST PRACTICE 2:

Authenticate Users Better

It's not uncommon for a third-party to lack the security maturity of larger organizations, and this is especially true for credential management. Vendor and partner credentials are often too weak and are susceptible to inadvertent disclosure. The best way to protect credentials is to proactively manage and control them.

Apply Multi-factor Authentication	Eliminate Shared Accounts	Enforce Onboarding/Offboarding Processes and Procedures	Use Background Checks and Identity Proofing

When someone joins a business partner's organization, an account is created and access is provided. That account and access must then be terminated when that individual leaves the company or changes role. To ensure such actions are handled in a timely fashion, automated vendor reporting of staffing changes is advised.

BEST PRACTICE 2:

Authenticate Users Better

It’s not uncommon for a third-party to lack the security maturity of larger organizations, and this is especially true for credential management. Vendor and partner credentials are often too weak and are susceptible to inadvertent disclosure. The best way to protect credentials is to proactively manage and control them.

Apply Multi-factor Authentication | Eliminate Shared Accounts | Enforce Onboarding/Offboarding Processes and Procedures | Use Background Checks and Identity Proofing

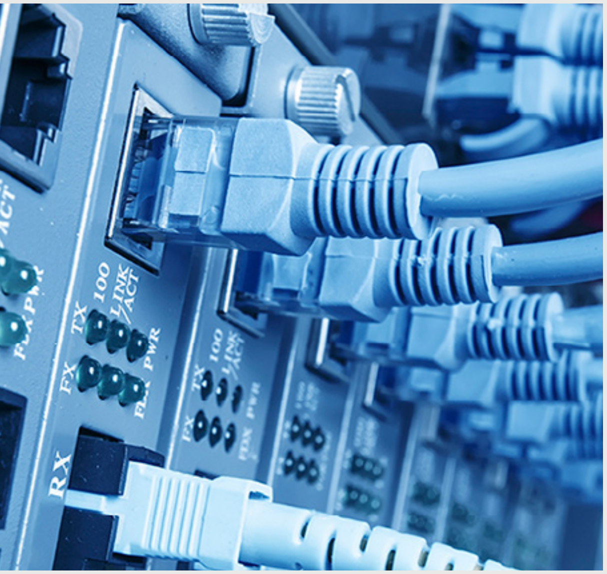
In very sensitive environments, the requirement for background checks and identity proofing of third-party individuals accessing systems is recommended. This can be costly and time-consuming, so it’s a risk management question. Given cases where third-party users have been shown not to exist (as part of a larger business fraud), it may make sense to undertake at least some degree of identity proofing.

BEST PRACTICE 3:

Separate Authentication from Access Control

Most vendors only need access to very specific systems. However, the typical network is not well segmented physically, which would help control access. As a result, should an attacker gain access, he or she has visibility of a broad range of devices and systems. And once inside, the attacker can search for vulnerabilities or additional credentials that can be exploited to gain more access, at a higher level of privilege—as was the case in the Target, Home Depot and Ukrainian Power Grid breaches. To protect your organization, network visibility and access should be limited using physical or logical network segmentation.

Physically Segment Your Network | Logically Segment Your Network | Channel Access through Known Pathways



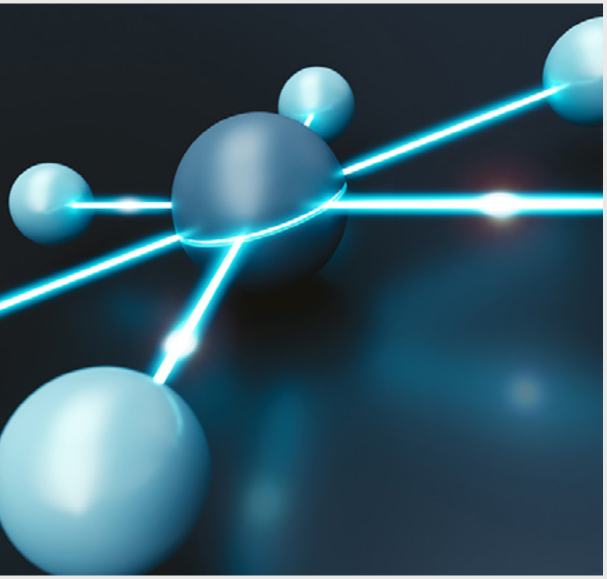
Though administratively intensive, physical network segmentation is required for certain regulatory mandates and is effective in limiting the scope of available resources.

BEST PRACTICE 3:

Separate Authentication from Access Control

Most vendors only need access to very specific systems. However, the typical network is not well segmented physically, which would help control access. As a result, should an attacker gain access, he or she has visibility of a broad range of devices and systems. And once inside, the attacker can search for vulnerabilities or additional credentials that can be exploited to gain more access, at a higher level of privilege—as was the case in the Target, Home Depot and Ukrainian Power Grid breaches. To protect your organization, network visibility and access should be limited using physical or logical network segmentation.

Physically Segment Your Network | Logically Segment Your Network | Channel Access through Known Pathways



Through the use of a privileged access management solution, you can specify what resources are available to a user and enforce these policies, limiting an individual to just those systems. Often, this logical segmentation is faster and easier to implement and maintain than physical boundaries. The user only sees the systems he or she is permitted to access. What's more, you can intercept and prevent the execution of specific network commands, such as TELNET and SSH, eliminating malicious lateral movement.

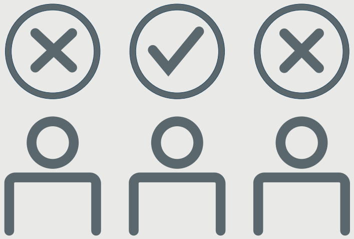
BEST PRACTICE 3:

Separate Authentication from Access Control

Most vendors only need access to very specific systems. However, the typical network is not well segmented physically, which would help control access. As a result, should an attacker gain access, he or she has visibility of a broad range of devices and systems. And once inside, the attacker can search for vulnerabilities or additional credentials that can be exploited to gain more access, at a higher level of privilege—as was the case in the Target, Home Depot and Ukrainian Power Grid breaches. To protect your organization, network visibility and access should be limited using physical or logical network segmentation.

Physically Segment Your Network | Logically Segment Your Network | Channel Access through Known Pathways

By defining acceptable paths for external access to resources, identifying anomalies becomes much easier. Using a privileged access management solution or VPN, you can contain unapproved protocols and direct approved sessions to a predefined route.



BEST PRACTICE 4:

Prevent Unauthorized Commands and Mistakes

Sometimes technical or administrative reasons may warrant a third-party user to gain access to systems using a highly-privileged, super-user account, like root or admin. With such unfettered access, that individual can cause significant damage—whether their actions are malicious or accidental. A better, and more palatable approach, involves using a privileged access management solution to enable fine-grained permission controls.

Enable the Safe Use of Administrative Accounts

Limit Commands a Specific User Can Perform

Facilitate Monitoring and Alerts

Using a privileged access management system, you can allow an individual to have sessions brokered on his or her behalf to various target systems using a number of different accounts, each with different permission levels.

BEST PRACTICE 4:

Prevent Unauthorized Commands and Mistakes

Sometimes technical or administrative reasons may warrant a third-party user to gain access to systems using a highly-privileged, super-user account, like root or admin. With such unfettered access, that individual can cause significant damage—whether their actions are malicious or accidental. A better, and more palatable approach, involves using a privileged access management solution to enable fine-grained permission controls.

Enable the Safe Use of Administrative Accounts

Limit Commands a Specific User Can Perform

Facilitate Monitoring and Alerts

tion v() {
var e = $("#use").val();
if (0 == e.length) return "";
e = k(",", " ", e), e = e.replace(/ +(?=)/g
for (var t = e.split(" "), l = [], s = 0;
return l
nction h() {
var e = $("#collected_ta").val();
e = k(",", " ", e), e = e.replace(/ +(?=)
for (var t = e.split(" "), l = [], s = 0;

Command filtering—using blacklists and whitelists—can provide a high degree of both control and flexibility. A blacklist contains commands that are not permitted, while a whitelist contains commands that can be issued.

BEST PRACTICE 4:

Prevent Unauthorized Commands and Mistakes

Sometimes technical or administrative reasons may warrant a third-party user to gain access to systems using a highly-privileged, super-user account, like root or admin. With such unfettered access, that individual can cause significant damage—whether their actions are malicious or accidental. A better, and more palatable approach, involves using a privileged access management solution to enable fine-grained permission controls.

Enable the Safe Use of Administrative Accounts	Limit Commands a Specific User Can Perform	Facilitate Monitoring and Alerts

By logging and monitoring a user's actions, the system can issue appropriate **alerts when policy violations are encountered**. Here are some of the possible responses:

- Block and warn the user
- Terminate the session
- Disable the user account
- Generate alert/alarm SOC

BEST PRACTICE 5:

Monitor and Investigate

In order to enforce established policies for system access, some level of monitoring is required. The specific level and scope of monitoring necessary depend on your risk and compliance management considerations. Even in environments with little risk, logging and monitoring a user's actions can help you capture suspicious activity and investigate the details to determine intent.

Capture Basic User Activity

Conduct Session Recordings

Correlate Logs and Alerts Generated by Network and Security Tools

A violation may be a simple mistake, or it could be an indication of malicious behavior. By keeping a basic log of a user's activity—logon and logoff times, systems accessed, commands issued and responses received—you can identify and **address inappropriate or unauthorized activity** and identify third-party users in need of additional training.

BEST PRACTICE 5:

Monitor and Investigate

In order to enforce established policies for system access, some level of monitoring is required. The specific level and scope of monitoring necessary depend on your risk and compliance management considerations. Even in environments with little risk, logging and monitoring a user's actions can help you capture suspicious activity and investigate the details to determine intent.

Capture Basic User Activity

Conduct Session Recordings

Correlate Logs and Alerts Generated by Network and Security Tools

For more sensitive environments, session recording may be needed to provide complete information about a given session. These sessions can then be **examined in cases of known policy violations** or problems that subsequently arose within a system.

BEST PRACTICE 5:

Monitor and Investigate

In order to enforce established policies for system access, some level of monitoring is required. The specific level and scope of monitoring necessary depend on your risk and compliance management considerations. Even in environments with little risk, logging and monitoring a user's actions can help you capture suspicious activity and investigate the details to determine intent.

Capture Basic User Activity

Conduct Session Recordings

Correlate Logs and Alerts Generated by Network and Security Tools

Relevant data about an enterprise's security is produced in multiple locations. Being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary.

The Key to Protecting Your Business

Whether they are obtained maliciously or leveraged inappropriately by a valid user, exploited third-party user accounts are a common thread in many data breaches. And as your ecosystem of vendors grows, so does the challenge of defending against such attacks. The Privileged Access Management suite from CA offers a comprehensive solution to help you define, automate and enforce the five best practices described in this eBook across your physical, virtual and cloud environments.

To learn more, visit: ca.com/privileged-access-management