

The background image features a person wearing a dark hoodie, holding a large US dollar bill. The image is heavily stylized with a digital glitch or pixelated effect, particularly around the edges and the bill itself. The overall color palette is dark, with blues and greys, and some orange/red highlights from the glitch effect.

SecureLink®

# The Anatomy of a **Third-Party** Data Breach

eBOOK

# The Anatomy of a Third-Party Data Breach

## CONTENTS

### Attack Methods

Most common ways hackers use third-party access	
Virtual private networks (VPNs)	
Phishing	
Malware and Ransomware	
Privileged credentials	
Top breaches that stemmed from a vendor or third party	
Target	
Hancock Health	
The Auto industry	

### The 5 Most Common Phases

Phase 1 Investigation: Choosing the victim	3
How to defend yourself	6
Phase 2 First blood: Attacking the vendor	6
Could your vendor(s) be vulnerable?	6
Common Worst Practices	7

Phase 3 Spreading the infection: Going after the healthy hosts	14
Defend yourself with credential management	14
Phase 4 Movement: Breakout or going lateral	16
How to properly protect yourself and your company	17
Intrusion Detection System (IDS)	17
Vendor management tools	17
Phase 5 Finale: Persistence or payday	18
Implement a well-rounded cybersecurity strategy	18

<b>The importance of a vendor access management platform</b>	<b>19</b>
Why you should care about vendor management	21
Lower the risks of cyberattacks	21
Quickly detect third-party data breaches	22
Fix third-party data breaches faster	22
Reduce the impacts of third-party data breaches	23
Do you have a vulnerable vendor?	23
Invest in your company's future	24

# Attack Methods

# The Anatomy of a Third- Party Data Breach: **Attack Methods**

We're not the first ones to tell you that hackers are breaching networks to steal data, personal information, and intellectual property, and we won't be the last. But, we might be the first ones to highlight the involvement that third parties, contractors, and vendors play in the world of data breaches.

In fact, the [Ponemon Institute and IBM](#) found that, in 2019, the cost of a data breach that involved a third party increased costs versus a data breach without a third party by more than \$370,000, or an adjusted cost of \$4.29 million. Additionally, out of the 26 different factors studied that contributed to a data breach, the involvement of a third party was the most expensive. Why? Probably because it is usually the easiest way for a hacker to get into a company; if a vendor is given privileged credentials to a company's server (or multiple company's servers) they can easily access a multitude of sensitive information. And it isn't just that there is one data breach a year, or some other



small or insignificant number of data breaches that involve a third party. In fact, [according to another Ponemon Institute study](#), nearly half (42%) of all data breaches involve a third-party or vendor.

The increase in data breaches and third parties being used as an “in” to servers makes a lot of sense and has become more common as companies outsource more work. The world has moved to more of an outsourcing model because of the fact that there are vendors that are really good at doing specific things, and they’re able to do these things remotely. Why have an onsite HVAC specialist when you could have someone who works for an HVAC vendor as a professional do upgrades and patches remotely? It’s just easier. Until, of course, you get hacked by an insecure vendor as Target did in 2013 in one of the largest breaches of all time.

One of the biggest reasons that data breaches occur, especially those that stem

from third party access, is due to the industrialization of the cybercriminal ecosystem and innovations such as ransomware, which make cybercrime much more profitable and easier to carry out. But with increased attacks and hacker infiltrations, there also comes increased laws and regulations. Remember when HIPAA “got teeth” when they introduced the HITECH Act? Third-party risk from these kinds of attacks started attracting the interest of both regulators and lawmakers. Third Party Risk Management (TPRM) is part of several major cybersecurity or privacy laws passed recently such as the GDPR in Europe, the CCPA in California, and the NYC-DFS in New York. With this focus on this type of risk, many companies have expanded or initiated vendor management programs to combat it. We expect that there will be more initiatives that move in this direction, too. Remember: you’re only as safe as your most vulnerable vendor.



**Remember:** you're only as safe as your most vulnerable vendor.

# Most common ways hackers use third-party access

**Third-party data breaches are so common because typically it's the weakest link that hackers can use in order to get into a network. What's better, for hackers at least, is if a vendor has access to multiple networks - then they can easily get a ton of information. Let's look at the most common ways, or paths, that hackers take.**

## VIRTUAL PRIVATE NETWORKS (VPNS)

VPNs are used by nearly every organization, especially with our workforces moving in the direction of working from home for half the time or even full time. VPNs were created out of a need to provide a connection to remote workers that behaved much like a local area connection. Your connection replicates the access you would get from work, but you get that access from the comfort of your house (or another location), but provides no additional functionality beyond access.

In other words, VPNs are a perfect solution to use for internal employees that need to access servers, files, or other resources that are specifically for internal

eyes. That's where the issue comes in: when VPNs are used by vendors, contractors, or third parties to access your network, rarely is that access fenced off to only the needed areas.

So maybe your vendor isn't a liability, but their access method into your network is. VPN access gives too much to vendors who only need a portion of said access in order to do their job. When VPN access is granted, the saying goes: it's not when a data breach will occur via that access, but when.

## PHISHING

We all say we would never get caught clicking a phishing email. We all know the typical emails where there are grammar issues, you need to send money to a Prince, or your CEO really needs your email, phone number, credit card information, and the name of your first born child (if applicable). Sure, all of these seem obvious to you and me, but that isn't the case for everyone. And hackers are getting more sophisticated with their phishing schemes and making them a lot more realistic. This is why phishing still works and will continue to work as long as humans are in front of the keyboard.

[It's been reported that phishing accounts for 90% of data breaches](#); that's not only a huge chunk of data breaches, but it's the vast majority of them. So we might all think that we're smarter than a hacker that uses phishing as their way in to a network, but that isn't always the case, even for sophisticated

users. Maybe you and your team can outsmart the phishing attack, but what about the other people you don't directly hire-- like those vendors, their support reps, and different contractors? And, if they have access to your network (especially if it's through a VPN or another platform that wasn't specifically made for vendor connections), you might already have a hacker in your system.

## MALWARE AND RANSOMWARE

Another typical thought pattern for a lot of us to rely on is that a malware or ransomware attack might happen, but it would never happen to me or my organization. Confidence is always great to have, but do you have the systems in place to back up that confidence?

Whether or not you have your answer to that question above, the statistics on ransomware are staggering. In fact, [Emisoft reported](#) that the cost of ransomware attacks surpassed \$7.5 billion in 2019. Along the same lines, [Datto reported](#) that downtime costs have increased 200% year over year. And both reports state the fact that ransomware isn't going away anytime soon. With ransomware being massively successful, why would hackers stop? They don't necessarily care about the data they can encrypt, rather, they care about the fact that

you care about the data or the intellectual property so you'd be more than happy to pay the ransom to get whatever they took or bring your systems back up, unencrypted. It's supply and demand: as long as we continue to keep our systems vulnerable to hacks like this and a company is willing to make the payments, ransomware is here to stay. It's up to you to ensure that your perimeter can handle it when the attack comes your way.

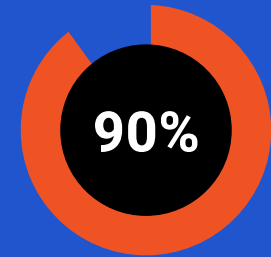
Data isn't the only thing that can get hacked with a ransomware attack. [Emisoft highlights](#) some that are literally life and death situations:

- » Emergency patients had to be redirected to other hospitals.
- » Medical records were inaccessible and, in some cases, permanently lost.
- » Surgical procedures were canceled, tests were postponed, and admissions halted.
- » 911 services were interrupted.
- » Badge scanners and building access systems ceased to work.
- » Schools could not access data about students' medications or allergies.
- » Power plants and gas pipelines have had operations interrupted and equipment damaged or tampered with.

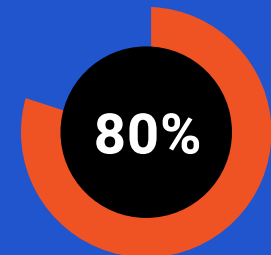
## PRIVILEGED CREDENTIALS

Just like data breaches, not all credentials are created equal. The access that each internal employee is given is created specifically for that employee, depending on their department, title, and need to access parts of a server. Privileged credentials, or administrative credentials, have access to everything and can unlock further privileges for other employees when necessary.

Here's the important part of privileged credentials: if you don't even give them to all internal employees, why would you ever trust a vendor with them? And, it doesn't even have to be the vendor that's the one that is the bad actor. Bad actors can use a vendor's (or supplier, contractor, or third party's) privileged credentials to wreak havoc in a small amount of time. You have essentially opened yourself up for a data breach or ransomware attack. And the facts back it up; according to [Verizon's Data Breach Report](#), 80% of all hacking-related breaches are tied back to privileged credentials.



**Phishing accounts for 90% of data breaches**



**Of hacking-related breaches are tied back to privileged credentials.**

# Top breaches that stemmed from a vendor or third party

**We see data breaches every day, if not more than one per day. You get sent something in the mail that says your information has been breached and that they're offering you free credit monitoring, but that they aren't sure exactly what information was taken. Maybe it was credit card information and your address, or maybe it included something like your social security number and medical history.**



**A credit card can always be canceled, your social security number cannot.**

Sure, not all data breaches are created equal. You might think some are worse than others, but the issue is that they're all bad, they're increasing in how often they're happening, and it's been reported that data breaches that involve a vendor are more expensive than ones that don't. So, it boils down to this: if a breach involves a third party or a vendor, expect to pay more in terms of money, downtime, and reputation.

It only takes one vendor who has access to your network to create a domino effect where your whole network goes down in flames, your company is making headlines for all the wrong reasons, and your PR team is scrambling to figure out how to spin it. And the worst part is, it's usually the vendor you least expect to be the entry point. Let's look at the most memorable breaches that have stemmed from vendors.

## TARGET

What would a list of vendor data breaches be without including the infamous Target breach of 2013? Perhaps the most famous third-party data breach to date, [Target's breach affected 41 million people and Target had to pay \\$18.5 million](#). But what exactly happened?

Target, like most companies, decided to use a vendor (Fazio Mechanical, to be specific) to handle their Heating, Ventilation, and Air Conditioning (HVAC) systems, that was a professional in their field. However, there was an issue with the relationship between the two companies. Target allowed Fazio to use a virtual private network (VPN) to remotely connect to Target's networks to maintain the systems remotely. Fazio was hit with malware via an email, and Target didn't stand a chance. What's important in this situation is the fact that Fazio Mechanical didn't even have access to the

point of sale (POS) system, but their VPN credentials gave them access to a project management file exchange which is all the hackers needed to expand their access and eventually hack other systems, including those critical systems. What made matters worse, was that this attack was discovered during the holiday season when retailers make most of the money. The resulting press coverage, fines, and lawsuits were catastrophic for Target's stock price and financial results for several years. Additionally, many members of the management team were fired in the aftermath.

## HANCOCK HEALTH

One of the top industries for hackers to target is the healthcare industry, which makes a lot of sense. Your doctor's office has a lot of information on you: your name, address, social security



number, reason for the visit, and more. It's a ton of data that's worth way more than a credit card number. In fact, [a Trustwave report found that personal health information \(PHI\) is worth \\$250 on the black market, when a credit card is worth only \\$5.40](#). A credit card can always be canceled, your social security number cannot.

In January 2018, Hancock Health was hacked and ransomware was installed on computer systems that locked critical files. And, as you probably guessed, this attack wasn't "through the front door." The group that installed the ransomware obtained the login credentials and used the "side door" of a vendors' access to Hancock's servers.

This brings up an important aspect of a vendor relationship: it would be great if vendors never have access to privileged credentials, but this isn't always a reality. In a perfect world, this would be accepted by all organizations, no matter the size. However, we don't live in that utopia-- and the statistics prove that. And don't forget: Verizon reported that 80% of all hacking-related breaches are tied back to privileged credentials. Again: this makes sense. Privileged credentials are the keys to the whole kingdom, not just a section or a room.

## THE AUTO INDUSTRY

What do Tesla, Toyota, Fiat/Chrysler, Ford, General Motors, and Volkswagen have in common? It's not just that you might drive something from them (or know someone who drives something by their

"But the inadvertent exposure of customers' data illustrates a problem confounding businesses: Some of **their biggest security risks come from their suppliers and contractors.**"

Stacy Cowley, New York Times

brands). It's that they had sensitive information and trade secrets breached because of a security error from a vendor they all had in common-- Level One. Having a vendor in common typically isn't a huge deal, but everything changes if that third party leaves a significant amount of sensitive and proprietary information on the internet, unprotected and visible to anyone looking for it.

This breach was first reported in July 2018, by The New York Times, and originally found by the cyber-risk researcher, Chris Vickery, from UpGuard. The data--roughly 157-gigabytes and nearly 47,000 files filled with factory records and diagrams--required no password or special permissions to ac-

cess. In other words, if someone knew where to look they could have access to trade secrets and other sensitive information from 100 different and highly regulated companies.

The exposed information contained:

- » Detailed blueprints and factory (e.g. assembly line) schematics.
- » Client materials including contracts, invoices, work plans, price negotiations, and customer agreements.
- » VPN access request forms.
- » Customer contact information.
- » Nondisclosure agreements.
- » Level One employee data, including driver's license and passport scans, ID photos, employee names, and ID numbers.

More often than not, enterprises spend a significant amount of money on internal cybersecurity efforts, but often neglect third-party security. This breach that affected many well-known car manufacturing companies highlights just that.

A person wearing a dark hoodie is shown from the chest up, looking down. A large, semi-transparent US dollar bill is overlaid on the image, positioned behind the person's torso. The background is a dark, textured blue.

# The 5 Most **Common Phases**

# The Anatomy of a Third-Party Data Breach: **The 5 Most Common Phases**

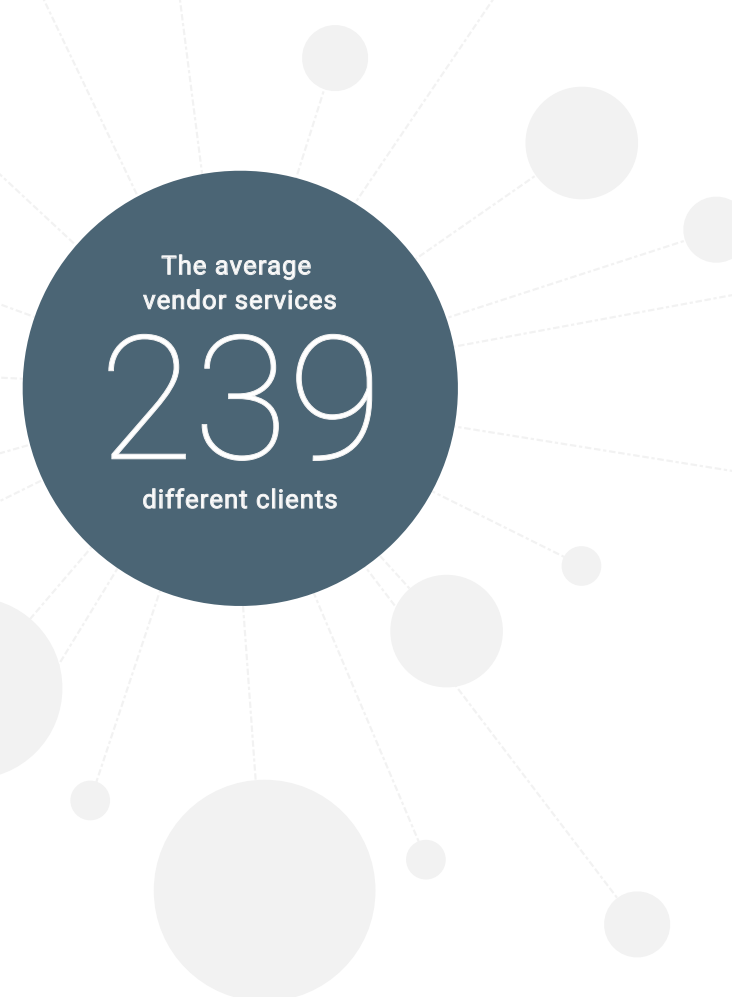
It doesn't take a whole lot of sophistication to figure out that you can go after a vendors' access to reach a larger company. Sure, you might not be able to get through the front doors of a major bank, but you might have more luck using a bank vendor's access to the bank's server to get what you want.

And hackers have seen a lot of "success" when using this route. It's well-known and widely accepted that vendors can regularly be smaller and less secure than a larger company that they service. So, they might have only a few (or no) IT resources or dedicated employees. Hackers see this, they take advantage of it, and we all read the headlines about the breaches.

The issue is, though, even if a vendor is bigger and well protected, it can still be worth it to a hacker. Instead of going after one company, vendors (regardless of size), can have access to multiple companies that have a wealth of information. [In fact,](#)

[the average vendor services 239 different clients.](#) So, if one vendor can get you access to over 200 different customers-- why would hackers ever take a different route?

While these incidents may have many differences in terms of industries attacked, size of companies, and the goals of the hacking, the complicated operations usually have several phases in common. It's worth while to examine these commonalities and the countermeasures you can take to eliminate vulnerabilities you may have in each phase of a vendor-related attack. For vendor management, the best offense really is a good (and streamlined and



efficient) defense.

**If you have controls in place at each of the different stages, your company is going to be much less likely to fall prey to a vendor-related breach and make headlines because of it.** Below, the stages that are associated with a typical vendor breach are outlined with the underlying weaknesses that were exploited and how to fix or avoid them.

**PHASE 1**

# Investigation: Choosing the victim

Any attack, large or small, sophisticated or simple, involves this step. The attacker is going to scope things out, just like how they do in real-world crime (and in movies). From any respectable heist movie you've seen, you know that just about everything has to be perfect: the locations of the cameras are known, the number of security guards have been documented, when security takes breaks or has a shift change, and more.

Those that forgo the in-person heist and go after a vendor digitally are no different. They might look for large customer lists or an industry that is prized by cyber criminals since there is a lot more than just money to be gained and the payout can be greater. In fact, hackers no longer have to even leave the comfort of

their desk if they don't want to and still see a great payout. [According to the Ponemon Institute in their annual cyber crime cost report, the average cost of cybercrime for an organization increased from \\$1.4 million to \\$13 million.](#) Through finding information on how much a hacker can make for each attack, hackers can cash in some pretty lofty paychecks, especially with the introduction and use of increasingly virulent ransomware.

Sometimes during this period, hackers discover a vendor with access to a wealth of information in the form of the number of clients they service. Then, the hacker will generally focus more attention and resources on that target. Sometimes this process will take weeks, or even months, to gather the right information.



---

**Vet your vendors properly to minimize network vulnerability.**

---

This can be done, usually, using low intensity scans and other stealthy ways of gathering more information on the chosen victim. Hackers can also rely on Open Source Intelligence (OS-INT) tools, which are free to access and download to gather data from public sources. This "low and slow" approach to survey, if you will, pays dividends in the form of the discovery of more potential victims with more data caches to be hacked.

**HOW TO DEFEND YOURSELF**

In this phase, an ounce of prevention is worth a pound of cure. Vetting your vendors properly can mean that you cross off the option of having a vulnerable vendor in the first place. Vendor risk assessments and regular re-assessments can catch issues before they can bite you. Also, while the intentions are good, allowing your vendors (or anyone else who has access to your network) to cite or list you as a customer on their websites might shorten the whole investigation period for hackers while they do their best to discover the possible backdoors into your network. It's better to keep these references offline or upon request so they can't be publicly searched by people who want to wreak havoc in your network.





## PHASE 2

## First blood: Attacking the vendor

Once hackers have chosen their vendor and done the necessary research, the next step is to find out what “worst practices” they’re committing. Some of the most common are: shared credentials (as we know, this is the holy grail for hackers), poor social engineering defenses and security awareness training, dated patches, and other basic information security mistakes.

Next, it’s time to choose how the attack should go. Depending on the vulnerabilities found, that will dictate what kind of attack is chosen. Perhaps it’s a custom-built phishing campaign, or even a “spear phishing” campaign where top leaders and key employees are specifically targeted with malware-filled emails with cleverly crafted subjects and content to click. Whatever was found during

the research phase will dictate which attack and route in will work best. They may try several of these, hoping one will work.

In any organization, with enough time and effort, most will fall to one or more of these techniques. In fact, chances are, at most companies, big and small, hackers can find something to latch onto.



### COMMON WORST PRACTICES

- Shared credentials
- Poor social engineering defenses
- Poor security awareness training
- Dated patches
- Basic information security mistakes

For example, the [Delta Airlines breach publicized in a nasty lawsuit filed by Delta detailed the poor security posture and general bad business practices used by a chatbot vendor for their support function.](#)

### COULD YOUR VENDOR(S) BE VULNERABLE?

Again, keeping an eye on your vendors is key to knowing if you have a weak link. This means implementing regular audits of records accessed and annual due diligence reviews. These are good practices to keep your data safe and ensuring your vendors are secure. Vendors should be able to provide records of their security programs, policies and procedures, as well as third-party

vulnerability scans, penetration tests, and audits.

Additionally, vendors should be able to show proof of regular phishing simulation tests and security awareness training. Otherwise, their support reps and technicians are probably prone to social engineering. This hypothesis is especially true at larger vendors with a lot of employees. On this flip side, if vendors have certifications or industry accreditations, that is further evidence that they’re a vendor you can trust with your networks, systems, and data.



**DOWNLOAD:** Top 3 Ways to Identify a Vulnerable Vendor Checklist

**PHASE 3**

## Spreading the infection: Going after the healthy hosts

Once they're in, novice hackers will often loot what they can get from the vendor and leave with evidence all around of their wrong doing, so the holes get patched up quickly. But serious or more well-trained hackers will sit back and wait until it's the right time to attack the customer that the vendor services. Even if they hacked the vendor by accident, not intending to go after the customers, they will soon realize they have breached a treasure trove of other potential victims.

Hackers will watch the network traffic while scooping up IDs and credentials, details on customers, and other useful data for the next attack. They're also going to map out potential paths into customer networks via VPNs and

other network connections. If they are really lucky, it's possible that they hit the jackpot: a dedicated connection with no firewall that leads straight onto a customer network.

If not, hackers still have options. They will just continue collecting intel until they have all the information that they need for the real attack on the vendor's customer list. It's also likely at some point, someone will log into the customer's network with a password in clear text. If not, hackers can comb the emails and hard drives of the vendor computers looking for credentials passed along in an email, chat, or stored in a spreadsheet. If that yields no results, internal wikis and ticket systems are also

fertile grounds to find this kind of information. Rarely does a hacker have to try all that hard to get to the information they want or need.

### DEFEND YOURSELF WITH CREDENTIAL MANAGEMENT

We can't be the first one's to tell you that your vendors should never have a single credential to spread to all their reps to log in with. Not only should all users have their own logins, but their access should be tailored to what makes sense: don't give the keys to the kingdom out to vendors who need access to a small portion of your network. Not so surprisingly, generic logins for a group of people, vendors or not, is never going to make a list of best practices. It's also going to get you



---

Rarely does a hacker  
have to try all that hard to  
get to the information  
they want or need.

---

in trouble with most compliance standards, like HIPAA, CJIS, and PCI-DSS. So, not only are you leaving your network essentially wide open to be hacked, but you're also opening your company's wallet open to paying off any compliance standards for being noncompliant.

Following these guidelines will limit the amount of sharing

and posting of credentials your vendors are participating in. Remember, you hired the vendor company, not all of its support reps so you don't know how security conscious they are.

To help with credential management, you should consider a credential management platform like Privileged Access Management (PAM). This branch of Identity and Access Management (IAM) technology allows you to take special care with your most valuable credentials, like the ones offering administrative control over systems. PAM systems have features that will store all of your privileged credentials in a secure vault, allowing only admins to check them out when needed. The worry of having to trust people with the actual privileged login and password is now removed from this process because PAM systems will log in for them and the password is never revealed



---

Leaving a wide open VPN connection into your network is essentially writing “steal me” on your car with the keys in the ignition.

---

to the vendor user. The credential vault will also frequently rotate the passwords and use extremely complex passwords that humans could never remember. We all know how hard it can be to remember passwords, especially when every platform has a different and unique one! And they should also have logging and auditing features so you can keep track of who is using what credentials, when, and for what servers.

We'd be remiss to not mention one of hackers favorite points of entry: VPNs. Keeping nailed up VPNs with vendors or business partners can be dangerous. This allows an intruder into a vendor network to seamlessly slide over into your network, without even needing a login. They can then explore your network at-will, looking for any vulnerable server or device to exploit for a permanent foothold to use as a beachhead for further attacks. If you must keep VPNs

always on for high traffic vendors, you should have a firewall on that connection with rules that dictate what servers can be contacted, on what ports, and, possibly, from what IP addresses in the vendor network. Leaving a wide open VPN connection into your network is essentially writing “steal me” on your car with the keys in the ignition.



#### PHASE 4

## Movement: Breakout or going lateral

Once the hackers have found a vulnerable host within your network to attach to, assuming they haven't immediately gotten into a useful server, they will look to expand their footprint in your network. Maybe they set up network sniffing to catch other passwords traveling over the network or probe other systems with scans, looking for vulnerabilities. With the information gathered off one network host, they can extrapolate network host names and usernames.

With network analysis tools, they can build a map of the network and identify servers they want to target. From there, they may take the direct approach and attack the target servers directly, or leapfrog from one system to the next on the way to the end goal. No matter

what movement they take, the longer they're in the customer network, the more systems they will get access to and the more data they will gather.

Breakouts can happen surprisingly fast. [A study by threat analysis company CrowdStrike showed that the average breakout time from initial entry to the next exploited system was under 20 minutes.](#) This means you have very little time, literally less than most TV shows on streaming services these days, from when an attacker first enters your network via a vendor to stop the attack from doing their damage.

In the famed Target stores hack, the attackers originally entered Target corporate via an HVAC vendor. Once in, they were able to quickly leverage an SQL injection



---

**By the time there are warning signs, hackers could have already been in multiple areas of your network over many months.**

---

attack to escalate privileges and jump over to their payment processing networks that handled transactions for all their stores. By the time there are warning signs, hackers could have already been in multiple areas of your network over many months, gathering over 40,000,000 customer credit cards.

This phase is also where a ransomware thief would make sure they infect as many machines as possible while also ensuring they target backups, too. They may utilize a vendor's own support tools to spread the infections faster, [like what happened when hackers used the ConnectWise tool deployed by a Texas managed service provider to quickly infect and lock up the systems and networks of 22 small city governments.](#) Having



protections in place to kill an intrusion before it becomes “septic” for your network is vital.

### HOW TO PROPERLY PROTECT YOURSELF AND YOUR COMPANY

A properly segmented network that uses firewalls and managed switches can prevent a lot of hackers from jumping around, or at the very least, it can prevent an outbreak from spreading further. Segmenting user workstations from server networks is the first step. For example, usually a marketing network doesn’t need to be able to talk to a development network. If there are exceptions, it’s better to deal with them on a case by case basis than to have a fully unsegmented network.

Other ways to segment by are location or by function (web servers versus databases). Some non-admin workstations will need to talk to core and critical servers; but if you design it to allow the

exceptions rather than “allow all” by default, you will be a lot better off security-wise. Servers that need company-wide access, such as Active Directory servers or mail servers, should be placed on their own segments and walled off from critical servers that don’t need it.

### INTRUSION DETECTION SYSTEM (IDS)

Another countermeasure against attackers moving laterally is having a well-tuned and monitored network-based Intrusion Detection System (IDS). These systems sniff everything on a particular segment and flag suspicious activity. Many companies use IDS technology at the network perimeter, monitoring what is going in and out of the segment. To prevent internal attacks, you’ll want one listening to critical internal segments as well. Attackers often get much noisier once they get past the

firewall with their scans and probes and an internal IDS could catch this activity.

### VENDOR MANAGEMENT TOOLS

For external access, you’ll want a dedicated tool like a Vendor Privileged Access Management (VPAM) platform that can allow for vendors to access only the systems they need to work on and never provides a raw network connection either to the host or to the network. This eliminates all but direct attacks on that server on the port the vendor was using.

**PHASE 5****Finale:** Persistence or payday

The endgame for these vendor-driven hacks depends on what their objective is. If it's simple data theft, they make off with your data as soon as they've collected enough of it to make it worth selling. More and more though, hackers are using ransomware so they can cut out the middleman and demand immediate payment for unlocking your data.

If they're using one of the Advanced Persistent Threat (APT) groups, they may decide to burrow in and stay a while. These groups are usually after something other than money: intel, intellectual property, or the future potential damage they can do once "activated" by some conflict or political action.

For example, some nation-state actors want to get into systems that control critical infrastructure like dams and power plants and then go dark. These "sleeper" agents wait for a war or other conflict to come alive and cause maximum damage to the systems or attached infrastructure.

**IMPLEMENT A WELL-ROUNDED CYBERSECURITY STRATEGY**

Monitoring and regularly auditing third-party activity, especially when it involves privileged accounts, can show signs of a breach even if the hackers are trying to be stealthy. With technology like Privileged Access Management for both internal employees and external vendors,

it's very hard for them to do anything at the administrative level without leaving traces in the logs. You should have a platform in place that keeps these kinds of detailed records and review them every so often to look for anomalies. Sometimes it will be


obvious, like a vendor accessing servers they are not supposed to be working on. Other times, you may have to dig for subtler signs of an intrusion.



---

**Implement a well-rounded cybersecurity strategy**

---



# The importance of a **vendor access management platform**

# The Anatomy of a Third-Party Data Breach:

## The importance of a vendor access management platform

The worst thing all of us can do is continue to sit back and watch third-party data breaches continue to make headlines without taking actionable steps to fully protect yourself, your company, and your customer's data.

We talk a lot about ensuring internal access security programs are up to snuff and making employees take security awareness training classes. We also send test phishing emails to see if anyone clicks, and update and patch software, when needed. But, what about the vendors, third parties, and contractors that you allow on your network? How do you make sure that they're on top of it and are always connecting with the safest and most secure method?

The best way is to put your trust into a vendor management platform because it's made for the job. Let's dive a bit deeper into that by talking about something we can all relate to: shoes. When you're picking out a new pair of shoes for a specific reason, you're going to do your research. Let's imagine you're running a marathon and you need shoes that can make it with you through the grueling 26.2 miles and you don't want your feet to hurt any more than they have to, right? You do your research, you ask your

friend who has been running marathons forever, and you also read online reviews to come to the conclusion of what pair to buy.

The reason painting this picture is so important is because you go through that process for just about anything you invest your money into and want it

to be the right product for what you're trying to accomplish or get done. You'd never run a marathon in a pair of sandals, would you? Similarly, you shouldn't be allowing vendors, third parties, or contractors to connect to your systems with products or tools that aren't made securely allowing vendors to connect. Let's take a look into the reasons why you should prioritize vendor management at your company.



**Just like you wouldn't run  
your marathon in sandals, you  
shouldn't allow third parties to  
connect via insecure methods.**



# Why you should care about vendor management

Not surprisingly, all reports and evidence highlight the importance that all organizations should put an emphasis on implementing a well-rounded cybersecurity strategy. An element which is regularly not included to the same extent as other programs are those that revolve around vendor controls and management. You regularly ensure that your internal access and security practices are current with cybersecurity best practices: no password sharing, changing your password every 90 days, and access to only what servers or files they need. But, this security is rarely implemented as completely with external entities like vendors, contractors, and other third parties.

The world continues to change daily and as new technologies and threats are introduced, those that embrace the change and need for an ever-evolving cybersecurity program will thrive and be able to handle whatever is thrown at them next, whether it's ransomware, a cyberattack, [or a group of teenagers in Florida looking at Slack messages to hack one of the biggest social media companies.](#)

The companies that understand the importance of implementing a tool specifically made for the control and management of vendors will see a marked improvement in four key areas that are not only costly, but avoidable, issues.

- » Lower the risk from cyberattacks that stem from a third-party
- » Detect third-party cyberattacks faster
- » Remediate cyberattack damages faster
- » Reduce impacts from those attacks

## Lower the risks of cyberattacks

In order to get the output of less risk from cyberattacks or other forms of breaches, you have to be willing to put in the inputs, or the necessary work, to see the results you want. Though it is relatively hard, if not impossible, to determine the exact number of attacks against your organization (even if your security posture would “win first place”), most attacks will be both unsuccessful and untraceable.

In fact, [in a recent Accenture report](#), proactive security leaders identified an average of 239 cyberattacks and non-leaders only identified 166 attacks. So not only are proactive leaders able to identify more cyberattacks, but that same report

also highlighted that leaders have a much higher success rate in defending against those attacks. Companies with a strong cybersecurity stance saw only 9 security breaches per year compared to 22 per year for other less secure companies. To break this down, this translates closely to four times the advantage in relation to dealing with security breaches.

No matter what sector your company falls in, this puts an emphasis on the importance of identifying all third party access (both technical and non-technical), controlling that access, and tightly monitoring and auditing who is accessing secure systems, data, and other protected processes. Again, the only way to be successful in this realm is to invest into a platform built specifically for the job. Just like you wouldn't run your marathon in a pair of sandals, you can't expect that a software that isn't specifically for managing and controlling vendor access will suffice.

# Quickly detect third-party data breaches

Similar to finding a burst pipe, the most important aspect of detecting a cyberattack is speed. The faster you're able to find a successful attack, the faster you can "stop the leak" and mitigate the damage by isolating the effects and fixing the issues. Detecting third-party data breaches quickly is the key to implementing any successful incident response.

Like we said, most companies do their best to be proactive by putting in the necessary work before a breach occurs. We all need to hope for the best, but expect the worst. In fact, the same Accenture report stated that 88% of the time, enterprise security leaders were able to detect a security breach, on average, in less than one day. The other 12% of leaders were able to

detect a breach in under a week. This means that for a large majority of leaders, security breaches were found almost immediately, and the full force of their security containment processes could be brought to bear within 24 hours of an attack. On the other side of the coin, companies that don't have a strong security posture are only able to detect an incursion within one day 22% of the time. The other 78% required more than a week to find breaches that affected their systems.

Often third-party data breaches go completely undetected by the enterprise and only get discovered when stolen data shows up for sale on the dark web or when a ransomware attack locks data away. And then the company's customers find out from a news report that their data has been breached, rather than from the company themselves, making a bad situation worse. In total, it's not a great look to have.


No matter what type of company you work for, early detection is going to be the key to success. If a breach is the cause of downtime, the longer it takes to find it and contain it, the longer the downtime continues. With many vendors entering and leaving your networks, systems, and devices multiple times, it's important to find any hole in the security as quickly as it happens so it isn't exploited more than once. And remember, you're only as secure as your most insecure vendor. If you have vendors

using a single, shared credential for their vendor reps, it's time to shut that down and implement a system that can ensure security and safety without compromising efficiency.

## Fix third-party data breaches faster

Once a breach has been found, the fight comes in two different forms: containing its spread and then eradicating the issue. The average time needed to repair a security breach and the speed of returning to "normal" are important aspects of cybersecurity resilience.

When dealing with a data breach, it's important to maintain business continuity while executing rapid return to operation (RTO) times. Most cybersecurity leaders are able to remediate a data breach in just over 2 weeks. But to do it completely, you must ensure that it never happens again. Patch any holes in your cybersecurity strategy and then hold detailed post-mortem strategy meetings with all levels of staff to review the incident and learn from what you and your company has been through. Embrace the mistakes, make changes, and do what you must to ensure a third-party data breach doesn't happen again.



No matter what type of company you work for, early detection is going to be the key to success.

The ability to plug cybersecurity leaks once they're detected is a crucial step to minimizing future breaches, especially when a breach comes from vendor access. You must be able to know, with granular detail, who is logging into the network, when, and how to help find any holes in your supply chain network security. If you can't say the number of vendors that have access to your network, and what that access consists of, it's time to visit your cybersecurity strategy as a whole.

## Reduce the impacts of third-party data breaches

Without the right tools in place, it really is the question of when and not if a third-party data breach will occur. Once you're affected by one, another important aspect of dealing with a third-party data breach is how much it impacts the business and how much you can reduce said impact. As noted earlier, the speed of recovery is essential in minimizing the damage of a breach, especially in relation to critical downtime. Being able to see what specifically was done means you can have a



Embrace the mistakes, make changes, and do what you must to ensure a third-party data breach doesn't happen again.

"blueprint" to the hacker's damage, making it easy to rebuild systems and find any backdoors and lock them out. Highly granular or high-definition logging systems for vendor activity is crucial to this effort.

Any impact that a third-party data breach has to your company is going to affect the bottom line. Limiting the damage of any breach is crucial to minimize the loss of revenue. As most companies outsource some of their work to a vendor or contractor on a regular basis, it's imperative to know what files or servers were accessed to ensure recovery is swift. Good audit and granular logs (the who, what, when, where, and why) can also greatly assist company security teams with forensic activity post-attack and prosecution, both civilly and criminal, of the bad actors.

## Do you have a vulnerable vendor?

Without being able to confidently say you know your vendors, what they access, when they access it, and you have proof to corroborate your "vendor facts", it might already be too late. But, a data breach by a vendor doesn't have to be the end all be all for your company. There's no day like today to invest in your company's future and success by implementing a well-rounded vendor management program with the technology to back it up.

If you're new to allowing vendors onto your network, or you plan to add new vendors, there are some red flags that can help you understand what you're getting into with a new relationship, like: have they been hacked before and do you have concerns over their lack of internal cybersecurity? There's no "silver bullet" that can save you from a data breach, but if you're proactive with your vendor's, asking the right questions BEFORE there is trouble, you're going to be in the best position possible if it happens

# Invest in your company's future

Maintaining security over devices, systems, and software is crucial to preventing downtime. Preventing security incursions by bad actors into the processes that run your company starts with controlling access by employees and vendors and ensuring that the access granted to each is different and made specifically for them.

It's important to control vendor access to guard against attacks in your network by limiting vendors' exposure to your network and systems. You need complete visibility into vendor access with a centralized vendor management platform. Know

which individual vendor reps are accessing your network, when they are entering the system, and exactly what activities they are doing.

In the event of issues or failures, being able to provide immediate and direct access to the vendor so that they can resolve the issue, while maintaining security and visibility, is crucial. The one thing we don't need is to give up efficiency to increase security; security and efficiency can work together, and the right vendor access management platform will allow you security, efficiency, and peace of mind.

Just like you wouldn't be caught running a marathon in sandals, don't allow your company to manage vendors and their reps with a platform that isn't made for the job. With SecureLink, your company can provide vendor companies and their reps with

---

The one thing we don't need is to give up efficiency to increase security; security and efficiency can work together, and the right vendor access management platform will allow you security, efficiency, and peace of mind.

---

secure remote access to networks, systems, and files while minimizing the downtime of any mission-critical systems, all while gaining visibility into and control over vendor remote sessions and their security.

## About SecureLink

SecureLink is the industry leader in critical access management, empowering organizations to secure access to their most valuable assets, including networks, systems, and data. By leveraging Zero Trust principles, machine learning, and artificial intelligence, SecureLink provides comprehensive security solutions to govern, control, monitor, and audit the most critical and highest risk access points.

Organizations across multiple industries -- including healthcare, manufacturing, government, legal, and gaming -- trust SecureLink to secure all forms of critical access, from remote access for third parties to access to critical infrastructure, regulated information, IT, and OT.