SECURELINK
VENDOR PRIVILEGED ACCESS

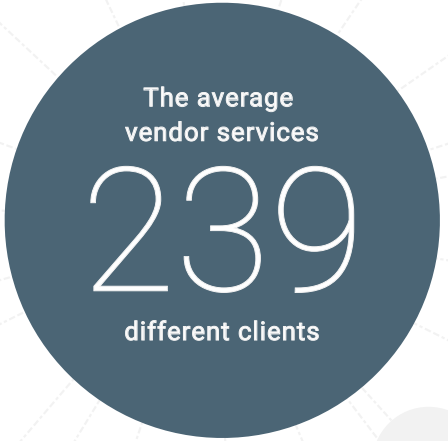
eBOOK

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

eBOOK

# The Anatomy of a Third-Party Data Breach: **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 outlines 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 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.

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

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 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.

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

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 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.

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

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**

# Continued reading

So, by looking at the different phases of a vendor driven attack and understanding the actions and motivations of potential hackers, you can take steps proactively to defend against them. Each phase is a potential both for vulnerability and countermeasures to be part of your "kill chain", if you will. Doing all these things will act as good defense in depth to protect your corporate castle from the vendor sourced data raiders.

**In Part 3, you will learn why a full vendor management program with the right tools is a necessity to implement in order to combat against the most typical phases of a third-party data breach.**

**About SecureLink**

SecureLink is the leader in managing vendor privileged access and remote support for both highly regulated enterprise organizations and technology vendors. SecureLink serves more than 30,000 organizations worldwide. World-class companies across multiple industries including healthcare, financial services, legal, gaming, and retail rely on SecureLink's secure, purpose-built platform. SecureLink is headquartered in Austin, Texas.

Interested in seeing how SecureLink can protect you from third-party data breaches? Get a customized demo today at **securelink.com/demo** or call us at **888.897.4498**



SECURELINK
VENDOR PRIVILEGED ACCESS