
WALLIX
CYBERSECURITY SIMPLIFIED
The Guide to Your Organization's Biggest Threat Vectors

The Guide to Your Organization's Biggest Threat Vectors

Corporate security teams spend a large amount of their time and resources attempting to secure their systems from outside cyberthreats – that is, from hackers who are external to the corporate network, and who have no business being there. Of course, it's prudent for security teams to do so: According to Verizon's 2019 Data Breach Investigations Report, almost 70% of confirmed data breaches are perpetrated from the outside.[1]

But what of the remaining 30% of data breaches? By a large margin, they were accomplished by employees acting from within their own networks. And of course, the objective of the external 70% is ultimately to gain internal access, making outside hackers into insider threats, too.

Accidental internal breaches are still breaches – and can come with a high non-compliance price tag

It goes without saying that any data breach is one too many – but with the high price tags attached to data breach mitigation and attendant regulatory non-compliance penalties, the avenues of risk are just too many for CSOs to ignore.

CSOs need to understand the varying kinds of data breaches that can come both from within and without their own organizations, particularly the threats posed by employees and contractors with admin rights and other elevated privileges. Some internal data breaches are accidental, of course, but that doesn't negate the company's responsibility to protect against them, either ethically or statutorily. On the other hand, some breaches are every bit as malicious as those attempted by external hackers. Regardless of intent and origin, however, it's important to know the potential threats – and how vulnerabilities can be closed.

DAMAGE DONE BY INTERNAL THREATS

Examples abound of data breaches caused by internal personnel, and the June 2019 data breach at North America's largest credit union, Desjardins Group, serves as a typical example. A Desjardins employee used his own credentials, as well as credentials he stole from co-workers, to obtain data on 2.7 million individuals and approximately 173,000 businesses. Although the employee was apparently not able to compromise customer PINs or passwords, he was able to get names, email addresses, transaction histories, and other information. Mitigating the damage from this breach has cost Desjardins 53 million USD in just the first 3 months after discovery.[2]

TYPES OF THREAT VECTORS

The Desjardins data breach wasn't particularly sophisticated because, occurring from the inside as it did, it didn't need to be. As the U.S.'s Cybersecurity and Infrastructure Security Agency points out, *"Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data"*[3] – and that's exactly why CSOs need to be just as vigilant about insider threats, not just those arising from the outside.

Remote Access

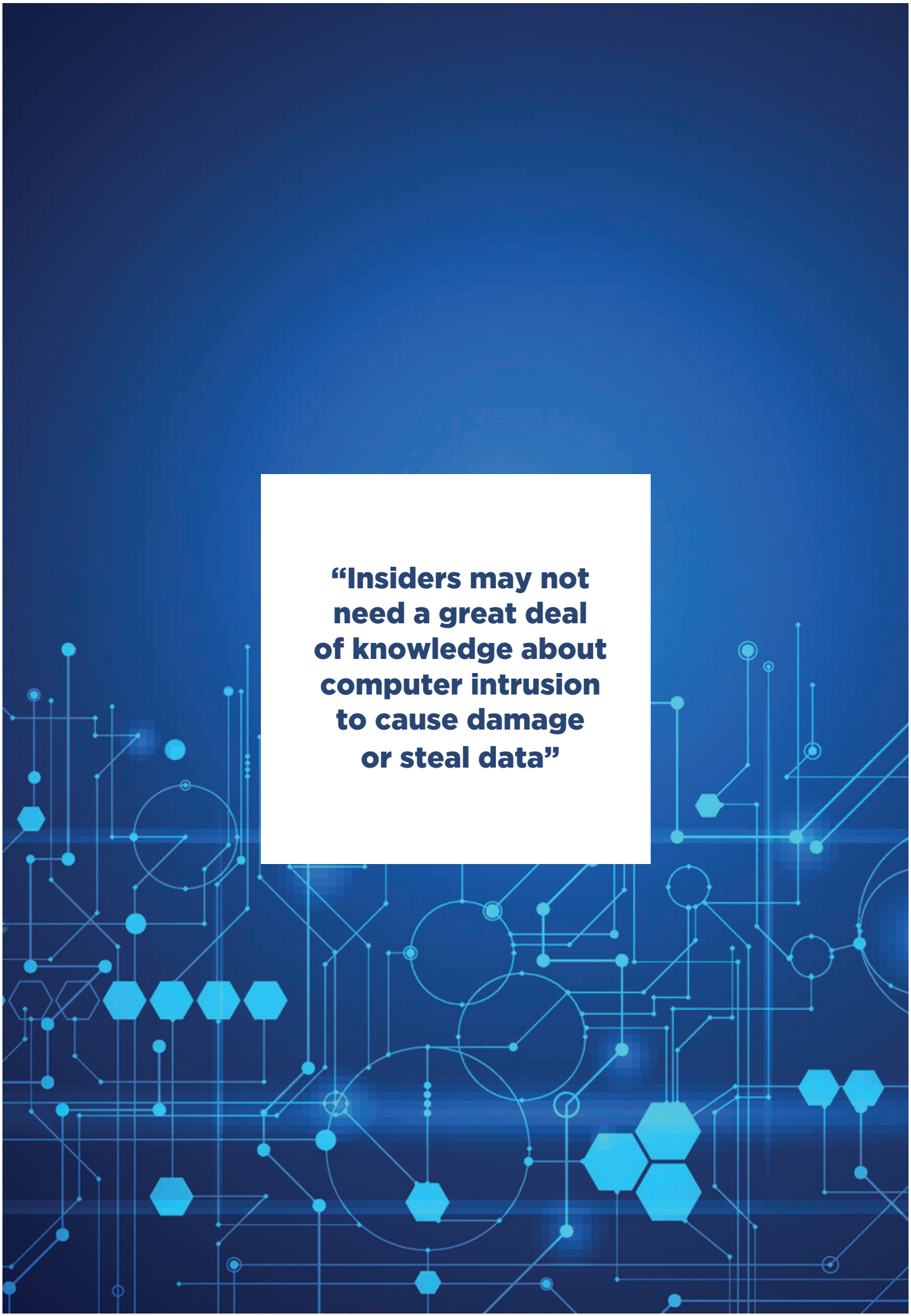
Privilege Abuse

Inappropriate Data Access

Unapproved Workarounds

Unapproved Hardware and Software

Education


“Insiders may not need a great deal of knowledge about computer intrusion to cause damage or steal data”

Remote Access

The modern workforce is diverse in many ways – including the many and varied remote workers and contractors who often access corporate systems to carry out daily tasks or one-off missions. The rise in the utilization of remote workers and contractors, though, has also given rise to a serious potential threat vector: Remote access doorways into systems.

The usual solution to this problem is to provide remote workers with a VPN access point, so that network traffic between the corporate network and the remote worker are encrypted. The use of a VPN, however, does not guarantee security: If a remote worker's machine is compromised by malware, for example, the malware could spread to the corporate network over the VPN. Likewise, with a machine that's been compromised in a way that allows hackers to control it: It becomes, via the VPN, a potential backdoor into the system.

To begin to address these particular problems, the company-side endpoint of the VPN connection is often a virtual desktop, instead of an actual machine. This works well if remote workers don't need access to other, privileged resources within the network. But if those privileged resources are accessible via the virtual desktop, the problem hasn't really been solved: Illicit users of the VPN connection will still be able to access any privileged resources they find on the network.

Access should never be unrestricted, but rather granted only to those resources where and when they are needed to accomplish a task.

As is often the case with cybersecurity, guarding against remote-access threat vectors requires more advanced measures. Requiring remote workers to use multi-factor authentication (MFA) is a good start, because it will help to ensure that the person logging in is indeed who they say they are. But beyond that, security administrators should be sure that remote workers do not have unfettered access to privileged resources. Any user – internal or remote – with high-level access to sensitive IT resources must have their access limited and controlled. This is the Principle of Least Privilege, which essentially posits that access should never be unrestricted, but rather granted only to those resources where and when they are needed to accomplish a task.

Privilege Abuse

One of the most basic threat vectors an organization faces is simple abuse of privileges. As the name suggests, privilege abuse involves

individuals taking advantage of the elevated privileges which they have been granted in order to do something they are not intended to do – access database records they don't need to see, for example, or accessing sensitive network systems they have no business in.

Because privileged users exercise their privileges in the normal course of their duties, this threat can be particularly difficult to deal with. The only real solution is to be sure that privileged access is not applied widely, authorized only for necessary resources and actions, and is both circumstance-dependent as well as closely monitored.

The only real solution for privilege abuse is to be sure that privileged access is both highly granular and closely monitored.

More precisely controlled privileged access helps by limiting who has access to which sensitive resources as well as the situations in which users can exercise their privileges. Granting access to one resource while blocking the visibility of other network resources the user has no need to see stops a wandering eye in its tracks. And, for example, if a database admin works only on weekdays and only from 9 to 5, granting access exclusively during those days and times can help forestall privilege abuse by denying access after work hours, when it is more likely to be used for nefarious purposes, or if the credentials have been lost or stolen.

But suppose an admin works alone on an overnight shift. In that case, they will need privileges that might be easily abused owing to the absence of other employees – which is why it's also important to monitor the activity that takes place within sensitive resources. With proper monitoring, every action taken while in session on a protected resource is logged and recorded, as well as their actions while in session. Furthermore, robust monitoring systems also include the capability to react, not just record – meaning that the session can be terminated instantly if the system detects an abuse of privileges.

Inappropriate Data Access

Closely related to privilege abuse is the threat of inappropriate access to – or handling of – data. A database developer may not need to be able to query every table within a database, for example, and a database admin may not need to be able to edit every database on a server. This is again the Principle of Least Privilege at work, stopping privilege escalation by granting a database developer specific privileges to a Customer table for legitimate work they are doing, but not to a Transaction table, which would allow them access to private customer information for which they have no need.

Such inappropriate access can – and does – lead to scenarios in which unauthorized actors gather vast amounts of personal and private information. Such data sets are extremely valuable to those bent on ill intent, as was the case with the Desjardins breach, because in the worst case they can enable things like fraudulent transactions – but even in the best case, they still expose victims of the exploit to identity theft and other lingering damages.

Furthermore, even if impact to the victims is minimal, damage to the company itself can be severe owing to the strong penalties (potentially millions of dollars) imposed by regulatory acts such as GDPR and HIPAA when privacy has been breached or security was found to be insufficient.

Inappropriate data access can be costly to a company, even if damage to victims is slight.

The answer to this threat is to be sure that privileged access is always as granular as possible. The aforementioned database developer may need query rights to the tables they work with during business hours, but their actions should be denied and their sessions terminated if they attempt to go beyond the scope of their privileges. Indeed, this granular approach should extend to all users requiring elevated privileges to critical IT asset preventing lingering privileges that could be taken advantage of long after work is accomplished.

Unapproved Workarounds

Finding loopholes and seeking efficiency is human nature. No long likes tedious or complicated processes to accomplish daily tasks. Though we all want to make our work as easy and as efficient as possible, loopholes and workarounds are a threat to security. For companies with cybersecurity systems that are cumbersome, at best, and place extra burdens on users, such systems are often circumvented not with ill intent, but for the sake of convenience.

If security measures slow users down or make their work more difficult, they're going to seek alternate routes.

A classic example is the creation and reuse of passwords across multiple privileged resources. When an admin is tasked with having to work with many such resources, it's much easier for them to create one easy-to-remember password and reuse

it across multiple privileged resources (or between multiple team members) than it is to create secure and distinct passwords for each resource. The problem, of course, is that easy-to-remember passwords are very often also easy to guess – and because the admin is unlikely to change passwords very often, they also create a vulnerability that spans all privileged resources on which they have been used. And when multiple people use one shared set of credentials, it's no longer possible to track which admin logged in and took which actions.

Passwords that are not often rotated, particularly if they are easy to guess, create a vulnerability that spans all privileged resources on which they have been used.

A similar problem arises with DevOps teams, well-known for seeking routes to efficiency, hard-code passwords in scripts. And, often, upload these scripts to GitHub thereby publicly publishing credentials to proprietary systems. While they may not mean any harm by streamlining their need to sending dozens or hundreds of logins as they work, DevOps habits can put your organization at risk.

The answer, of course, is that password vaults and password management tools should be easy for admins to use without hindering them in the performance of their tasks. Enforced password rotation, Application-to-Application Password Management (AAPM), and robust password vaults go a long way to implementing efficient security. The only effective cybersecurity tools are those which are actually used, and the only tools which will be actually used on a regular basis are those which don't hinder admins from doing their jobs.

The only effective cybersecurity tools are those which are actually used.

Unapproved Hardware and Software

Like unapproved workarounds, admins and other privileged users who use unapproved devices or software typically do so for the sake of convenience, not ill intent. The threat that these devices and software pose from the inside is real in large part because they have not been vetted or, in the case of hardware, does not have proper security software installed. This, in turn, leads to a situation in which privileged users bring compromised devices or flawed software inside of external security measures – and bring access for hackers with them.

Aside from tighter controls implemented via corporate Bring Your Own Device (BYOD) policies, the inside threat from outside devices can be mitigated by ensuring that well-implemented privileged access management (PAM) tools are in place to guarantee that IT asset protection remains regardless of the device being used.

But because potential malware might already be in such devices, real-time session monitoring is of critical importance to record and alert for suspicious session activity, since a hacker might be able to use an admin's laptop to access privileged resources without anyone being aware that such activity is occurring. Real-time session monitoring helps to mitigate this threat by being constantly on the lookout for unusual session activity and enables security teams to take immediate – even automatic – action if need be.

The need for such real-time session monitoring also holds true in cases where privileged users are using their own software. Because such software has not been vetted by the security team, it might contain backdoors that open access to hackers from inside corporate firewalls and other protections that might be in place. And because the software will not be an endpoint in its own right, monitoring all session traffic for suspicious activity is a key component in protecting against threats brought inside by unapproved software.

One More Key: Education

Across all threats, the key to protection is a combination of granular privileged access control and constant, real-time monitoring. No matter the source, all threats ultimately become insider threats with hacked, lost, or stolen access to critical assets. Such a combination is vital in ensuring that the biggest threats from the inside or outside – admins, remote workers, partners/contractors – are minimized in their ability to inflict damage, whether intentional or not.

But there's another key element to this defense: Education. By educating privileged users on security measures and threats, including the fact that sessions are monitored in real time, as well as recorded and preserved for auditing and accountability, some potential threats can be headed off simply because would-be bad actors are aware of the high probability that they will be caught, and will be unwilling to take the risk.

By educating employees on what it means to have privileged access, potential breaches might be avoided as users will exercise more caution in using their privileges.

The Bigger Picture

When discussing cyberthreats, it's important to remember that the goal of every hacker is in fact to penetrate external defenses – and once they've achieved that, they have turned, in important ways, from an external threat to an insider threat.

Thus, proper cybersecurity against all threats requires certain key elements: Granular privileged access control, session monitoring and alerting, and strong password management tools. Privacy of data is a right that's encoded in GDPR, HIPAA, ISO 27001, and many other cybersecurity regulations and guidelines – and it's only through properly managing cybersecurity that the privilege of accessing that data, when needed, can be protected no matter the threat vector.

Resources

[1] 2019 Data Breach Investigations Report. Verizon. Retrieved from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[2] *"Canada's Desjardins Reports Costs of $53M Related to Data Breach."* Insurance Journal. Retrieved from https://www.insurancejournal.com/news/international/2019/08/13/535593.htm

[3] *"Cyber Threat Source Descriptions."* U.S. Department of Homeland Security, Cybersecuirty and Infrastructure Security Agency. Retrieved from https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions

about WALLIX

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED