Insider Attacks:

The Unknown Threats to Today's Organizations

Untethered Labs, Inc.

Dr. Sid Potbhare &
Cecil B. Clarke, CISSP

info@gkaccess.com

White Paper – Issued 2021

GATEKEEPER

240-547-5446
info@gkaccess.com
gkaccess.com

Abstract

Each year, millions of organizations and individuals in the United States fall victim to a data breach. Forecasts from the Identity Theft Resource Center predict the total number of compromises to hit an all-time high in 2021. (1)

Organizations are aware of these risks, and most invest in cybersecurity defenses engineered to combat malicious outsider threats. McKinsey research confirms that 75 percent of experts across industries consider cyber risks to be a chief concern. (2) "As we've come to realize, enterprise security doesn't begin with the firewalls, LANs, and encryption – these are just tools (but very good tools). Policy, efficient training, and awareness of such issues provides the necessary foundation for strong security principles, implementation, and ultimately competitive advantage. Without training and proper knowledge of best practices, end users will never be able to properly use the tools provided to help them." says Cecil Clarke, CISSP.

Threats come in many forms, but fundamentally, they aim to gain unauthorized access to secured information. Cybercriminals then use that information to elicit harm to employees, the organization, or both.

However, data, employee, and organizational protection is typically focused outwards. Risks posed by insider threats are often unknown, unacknowledged, or second priority. But as employment arrangements shift in the wake of the pandemic and with almost half of the US labor force working from home, insider threats have fast become a new linchpin the modern-day enterprise. (3)

Remote work technologies and greater reliance on online and cloud-based software have transformed the dynamics of insider threats. This paper explores these insider risks in detail and highlights the tools and processes businesses can implement to mitigate insider risks and thrive securely.

Table of Contents

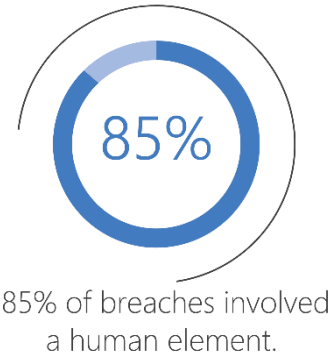
240-547-5446
info@gkaccess.com
gkaccess.com

240-547-5446
info@gkaccess.com
gkaccess.com

Introduction

Whether an organization's employees are returning to physical offices or embracing remote or hybrid work arrangements long-term, leaders must be cognizant of the dangers lurking within the company.

Preventative measures like firewalls, antivirus solutions, access controls, physical locks, ID cards, and password protection are vital to maintaining a strong security posture, and enterprises are spending big to uphold best practices. In 2021, the cybersecurity market is expected to surpass US $54 billion. [4] Yet, these conventional defense mechanisms may not adequately protect sensitive data against the simplest vulnerability in every organization – insiders. According to Verizon's 2021 Data Breach Investigations Report, 85 percent of breaches involved a human element. [5]



Average cost of a data breach worldwide is **$3.86 Million**

Insiders are in a prime position to steal data or unintentionally enable protected data to be exposed. And when this happens, the consequences are dire; the average cost of a data breach worldwide is $3.86 million. [6] For small and medium-sized companies especially, this can have a detrimental impact.

Insider threats can be classified as intentional or unintentional and divided into five distinct categories:

1. **Insiders who are malicious** – These actors are insiders who act against the organization's best interest purposefully for personal gain.
2. **Insiders who are disgruntled** – These individuals are chasing a personal vendetta against the company.
3. **Insiders who are careless** – These employees are not exposing company data knowingly. However, they are not diligent in their handling of protected and proprietary data.
4. **Insiders who are used as pawns** – These people are do-gooders yet are manipulated by malicious or disgruntled threat actors.
5. **Third parties** – More than half of senior leaders report an increased reliance on third parties, but just 28 percent continually monitor associated risks. [7]

Malware vs. Social Engineering Threats

Traditionally, organizations placed heavy emphasis on physical solutions (e.g., turnstiles, CCTV cameras, locks, fences, security officers, etc.). Today, new technologies have enhanced how companies approach perimeter defenses.

240-547-5446
info@gkaccess.com
gkaccess.com

While these protective measures make it more difficult for an outsider to breach an organization's network in a typical malware attack, malicious insider entities are better positioned than ever to leverage social engineering. This simple tactic empowers hackers to sidestep high-level firewall and antivirus security. Instead, they pinpoint weaknesses in human negligence, familiarity, and trust to trick employees into divulging information. From there, they gain access to virtual and physical corporate networks.

Examples of physical detective solutions:	Cameras, CCTVs, physical access control systems.
Examples of physical preventative solutions:	Fences, locks, dogs, security people.
Examples of technical corrective solutions:	System backups, restores, patches.
Examples of technical preventative solutions:	Encryption, layered security (2FA), Intrusion Prevention Systems (IPS).
Examples of technical detective solutions:	Audit logs, Intrusion Detection Systems (IDS).
Examples of compensating solutions:	Policy, training, awareness.

Social engineering uses psychological manipulation to draw credentials and other sensitive information out of unsuspecting individuals. For example, an attacker might phone an employee claiming to be a part of the organization's IT team and ask for a password. A legitimate-looking phishing email may be sent to an employee, prompting them to open a file, download an attachment, or click a link that contains malware. An 'urgency tactic' may also be employed. In this case, the attacker frames the situation as an emergency – if the employee fails to act fast, something detrimental will happen to themselves or their organization. Naturally, people aim to protect themselves and their company. Therefore, they are inclined to do as instructed.

Further, on-site social engineering involves a trusted visitor or employee. Because trust is implicit and pre-established, the likelihood of a successful breach is higher, and the outcome can be catastrophic. As the saying goes, *'When you give them an inch, they take a mile.'* CEO of Untethered Labs, Dr. Sid Potbhare, who works with many clients to upgrade their security remarked "The number of clients that are deploying 2FA *after* an incident rather than before is growing at an alarming rate."

Many organization leaders believe that employees can be trusted with all data. Or they fail to consider their data a valuable asset and, consequently, a hot target for cybercriminals. Businesses must invest the same resources into protecting against social engineering and corporate espionage (threat agents coercing insiders to disclose

240-547-5446
info@gkaccess.com
gkaccess.com

proprietary information in return for financial compensation) threatening critical data as they do petty thieves stealing physical assets.

How Attackers Gain On-Site Access and Steal Information

Security badges and ID cards may be effective in protecting against physical theft. They are not, however, impenetrable. All it takes is one courteous employee to unknowingly assist a criminal or ex-employee by holding the door open upon entry. This act of common decency can endanger the organization's security.

Tailgating, also known as piggybacking, is one way threat actors gain unauthorized entry into a company's physical premises. If there is no security guard on stand-by, the criminal walks closely behind a legitimate employee. When the employee uses their swipe card or enters a PIN, the criminal walks into the building behind them. In some cases, the criminal may have their hands full, subtly signaling to employees that they need help opening the door.

To many employees, their swipe card or security badge is nothing more than a key that grants them entry into the building. However, for security personnel, badges are a vital auditing system and mechanism for keeping track of who enters and leaves the premises. The information garnered from security badges can also assist a forensic investigation where needed.

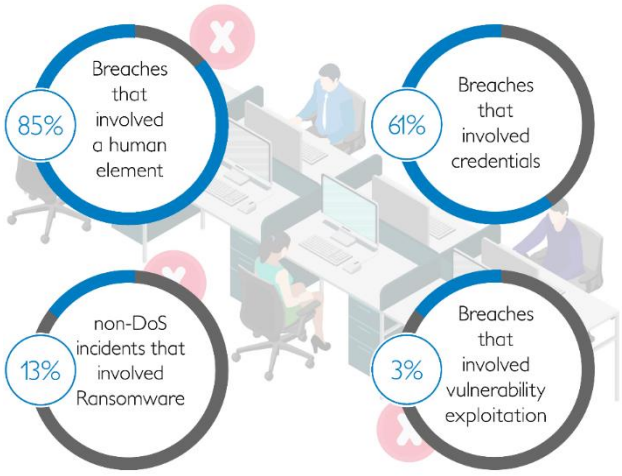
Mantraps are an effective mitigation strategy against tailgating. These involve a second security checkpoint upon entry – such as a physical key or security guard. However, mantraps can cause bottlenecks during peak, high-traffic times and can be costly to manage, so they may not be suitable for all organizations.
Once inside the building, criminals employ a technique called shoulder surfing to uncover credentials, personally identifiable information (PII), and other sensitive data. Shoulder surfing sees the attack wander throughout the office, peering over employees' shoulders at their computer screens. It's worth noting that shoulder surfing is not a tactic reserved exclusively for outsiders. Malicious or disgruntled employees can also steal information using this method.

After an attacker obtains passwords or PII from an employee's screen, they may wait for the employee to leave their desk. The criminal can then jump onto the employee's machine, log into the system, steal further

240-547-5446
info@gkaccess.com
gkaccess.com

information, and commit malicious acts. Breaches can escalate quickly, and the attacker's identity is firmly hidden.

Mantraps and other high-level security policies can limit visitor entry and activity, but organizations can never stop people from viewing others' desktop data. They can, however, implement robust defenses that lock desktops when the user is absent and strategically position monitors so that they are not visible to passers-by.



Source: Source: Verizon 2021 Data Breach Investigations

The Cost of Social Engineering

Social engineering can have devastating and long-lasting ramifications – the scope of the breach and the organization's response are two integral factors influencing the attack's outcome. Potential consequences include:

- **Downtime** – When a breach is in progress, an organization may lose access to its network. According to Gartner, downtime costs $5,600 per minute. [8]
- **Poor customer service** – Downtime affects your customer services team's response times, which could leave waiting customers frustrated. This is particularly dangerous in healthcare, for example.
- **Lost customer trust** – If a customer's PII is exposed during a breach, that customer may lose confidence in the organization and take their business elsewhere.
- **Poor staff morale** – If an unknown insider executed the attack, team members may become suspicious of one another. Trust is broken.
- **Potential legal ramifications** – Many industries are subject to data regulations and governance. If a breach is successful, the organization may be liable to a penalty or face a lawsuit.

Automated Authentication Solutions

Employees are a company's first line of defense. Therefore, cybersecurity awareness and education are vital. However, an educated employee may still let an attacker into the office – where humans are involved, human error follows since we're fallible. The risk of a data breach remains high, but there are several robust solutions available on the market that help reduce the threat of insider and social engineering attacks.

240-547-5446
info@gkaccess.com
gkaccess.com

All computers and electronic devices must be locked and secured when not in use. Employees may be aware of this best practice, but that does not mean they will follow it diligently every time. That is where automated, proximity-based authentication solutions come into play. Proximity-based authenticators automatically lock the desktop when employees leave their desks. Not only do these highly effective security solutions protect critical data, but they also relieve employees and administration from the burden of additional policies.

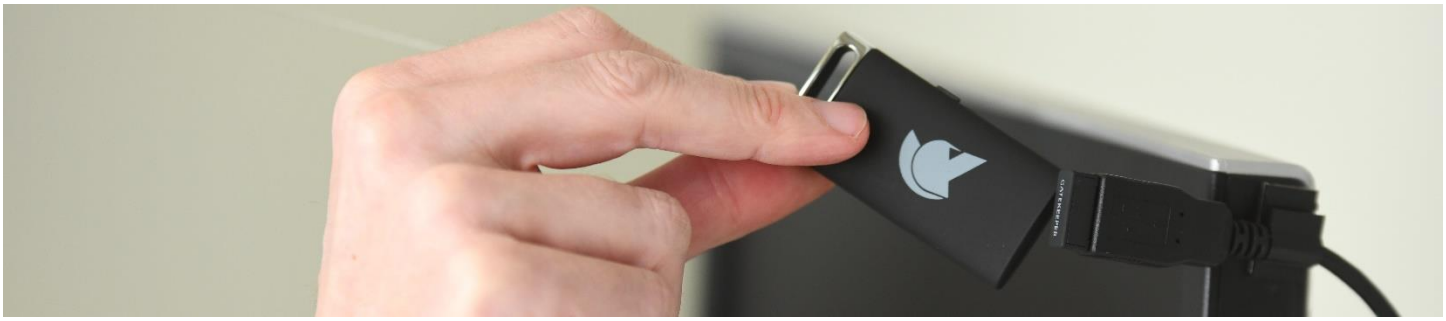
Utilizing continuous authentication, GateKeeper automatically produces detailed audit logs from every computer on the network, identifying the exact time when a user logs in and out of the computer. The solution uniquely identifies users using individually assigned tokens. Furthermore, audit data also includes information on applications and websites the user logged into during their session. These logs can be automatically forwarded to tools like Splunk for further analysis, including detection of non-standard and/or unauthorized access. By applying specific rules for authentication, GateKeeper can be configured to either prevent logins outside of work hours or require additional authentication for such use cases. Finally, through the proximity locking capability, any unattended workstations are automatically secured, thereby preventing malicious use of a user's account on any computer.

Conclusion

Employee education is vital in any organization's cybersecurity strategy, but it is not enough. Even the most educated employee can fall for a scam – especially where social engineering is involved. It takes just one lapse in concentration or one act of courtesy to expose a company's data.

A robust security policy must have limitations in place that manage employee and visitor behavior. Companies should also leverage proximity-based authentication hardware to auto-lock desktops to prevent visitors, employees, and unauthorized outsiders from snooping on attended and unattended devices. Otherwise, the risks of data loss, fines, lawsuits, restitution, and brand damage are real.

If you would like to learn more about the benefits of proximity-based authenticators and schedule a live demo, please contact the GateKeeper Enterprise team at 240-547-5446 or info@gkaccess.com.



240-547-5446
info@gkaccess.com
gkaccess.com

Citations

1. Data Breaches are Up 38 Percent in Q2 2021; The Identity Theft Resource Center Predicts a New All-Time High By Year's End, Identity Theft Resource Center
2. Safeguarding Against Cyberattack in an Increasingly Digital World, McKinsey
3. Stanford Research Provides a Snapshot of a New Working-From-Home Economy, Stanford News
4. Worldwide Cybersecurity Spending, Statista
5. 2021 Data Breach Investigations Report, Verizon
6. Cyber Crime Security Overview, Statista
7. Gartner Says Data and Cyber-Related Risks Remain Top Worries for Audit Executives, Gartner
8. The Cost of Downtime, Gartner