Whos On. Location

White Paper

Cybersecurity:

Managing the Insider Threat with Visitor Management

www.whosonlocation.com

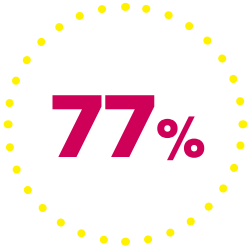
Introduction

The frequency, sophistication, and damage of data breaches due to cyber-attacks continues to escalate regardless of an organizations´ size and industry. These attacks cause organizations to lose customers, revenue, reputation, and operational continuity. While some organizations find data breaches costly, for others the damage can prove irreversible.

Due to the increased risk of cyber-attacks, data protection is becoming an increasingly important factor for organizations worldwide. And while most organizations have started to invest significant amounts of resources in improving their cyber security, many organizations fail to consider the risks associated with insider threats.

The risks by those who are invited to organization´s premises, such as visitors and contractors, as well as employees who are already there; are real and need to be addressed. To do so, organizations need to incorporate both physical and cyber threats into their data protection strategies.

The cost of a data breach



Percentage of U.S. businesses that have suffered between 1 and 5 separate incidents of data loss, leakage or exposure in the past 12 months.

In a recently published annual Cost of Data Breach Study by IBM and The Ponemon Institute, the global average cost was found to be $141 per lost or stolen record.

The study included 419 organizations in 13 countries with the highest average cost per record was the United States at $225 and Canada at $190. On average, organizations in India, the Middle East and the United States had the largest average number of breached records.

Additionally, the cost of lost business is highest for U.S. organizations ($4.13 million). This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

According to the same study, organizations in the Middle East and Canada have the highest direct costs and U.S. organizations have the highest indirect costs. Direct costs include resources spent to accomplish a given activity such as engaging forensic experts, hiring a law firm or offering victim identity protection services. Indirect costs involve the allocation of resources, such as employees' time and effort to notify victims and investigate the breach. Indirect costs also include the loss of goodwill and customer churn.

The threat from within

The reputational, financial and regulatory consequences of a data breach can be disastrous. Basically anyone who gains physical access into an organization can exploit security weaknesses and cause millions of dollars of damage. To mitigate this risk, organizations need to have a solution in place that will protect their IP and other critical assets from malicious insiders.

What is an insider threat?
Insider threats happen when an employee, contractor, or a visitor, who has or had access to an organization's network or premises, uses that access to compromise the confidentiality or availability of an organization's network, data or premises. Insider threats include fraud, theft of IP and data, espionage and sabotage.

"Between human error and malicious insiders, time has shown us the majority of data breaches originate inside company walls. Employees and negligence are the leading causes of security incidents but remain the least reported issue."

– Experian Data Breach Industry Forecast

Although cyber defenses play an important role in protecting from insider threats, it is important to note that malicious insiders are not only an IT issue. To mitigate the risk, organizations need to take an enterprise-wide approach to plan, prevent, detect, and efficiently respond to insider threats. Therefore, organizations need to address the gap between physical and digital security. To do so, there are several challenges that need to be addressed:

- *Insiders are often hidden in plain sight and are difficult to detect*
- *Insiders already have access and knowledge about the location of critical assets*

The business case for Visitor Management

Organizations in the US face threats nationally and internationally. And while most of them have started to invest in resources to upgrade their cyber defenses, a good portion of them do little or nothing in securing their doors and lobbies against malicious visitors, contractors, and employees.

34% of security incidents are attributed to insiders, including trusted third parties & employees.

Without a comprehensive and effective physical security plan empowered with visitor and employee management, organizations are at a constant risk from their visitors, contractors and employees accessing and stealing their IP and other sensitive types of data.

Ensuring that all available security measures are in place to protect an organization´s critical asset has become more important than ever. And as awareness surrounding data privacy and breaches continues to evolve, organizations struggle to accommodate the interests of numerous factions: individuals, government agencies, law enforcement, and national security agencies.

Therefore, organizations that do not keep track or log their visitors, contractors, or their employees, face significantly higher risk of a data breach.

How WhosOnLocation helps?

Besides being able to control visitors entering and leaving through different access points, organizations need to have detailed access logs in the event of a security breach. Paper and pencil manual log books are time consuming, challenging and prone to errors. WhosOnLocation´s People Presence Management application makes information about employees, visitors, and contractors easy to find and available in real-time. Accountability is important not just for security but also for safety reasons. This is why WhosOnLocation comes with evacuation management and hazard awareness features to account for visitors, contractors and employees during an emergency.

Making the connection: Merging physical access controls and digital security

Having a physical control on all entry and exit points is something that most organizations are familiar with. However, integrating these control mechanisms with organizations´ digital security systems does not only strengthen the overall security but it also helps save time and money. In a world where data breach due to insider threat is not a question of who but when, visitor management has become a critical component in the overall security of protecting your organization. WhosOnLocation´s People Presence Management enables organizations to streamline and secure their visitor, contractor, and employee management processes.

Centralizing security

Digital people management offers the possibility to control access and permissions across multiple locations from one simple and intuitive platform. Security and management can keep track of everyone who enters and leaves the facility, control access rights for different areas, as well as standardize access and security procedures across different locations. WhosOnLocation enables security and management personnel to view visitor details, assign badges and change their permissions.

"The world of business is becoming more uncertain, as with new system architectures come new cyber threats. No longer can the mechanisms deployed in the past be relied on for protection"

- Nick Gaines, Group IS Director, Volkswagen

Accountability

With no downloads and installations of any kind, WhosOnLocation´s Visitor Management removes the gap between physical and digital security.
With a portfolio of different starting plans and monthly or annual options, WhosOnLocation enhances safety, improves and centralizes visitor management, and increases organizations´ overall resilience to data breaches due to insider threats while saving you money, reducing your inventory, decreasing operational interruptions and streamlining your supply chain.

Conclusion

As discussed above, there is no reason for anyone to be able to enter or leave a company and wander the premises without being recorded and tracked. Organizations that do not have a well-planned and streamlined visitor, contractor, and employee management processes often rely on receptionists and sign-in books. Despite being time-consuming and prone to errors, these sign-in books are easy to bypass as receptionists can be easily distracted, especially in organizations with high number of visitors and employees.

In recent years, insider threats and overall risk of data breach has become a prominent issue. The change to a more flexible and open workplace environment has allowed visitors and employees to easily gain access to areas that are above their security clearance. While this risk continues to grow, organizations are slow in deploying additional security measures to mitigate that risk. The main reason for this is that organizations do not want to invest their resources in securing their IP and data since they believe the frequency of such threat is still very low, although the statistics show otherwise. Therefore, keeping track of visitors and their behavior is the key to determining and preventing insider threats.

A comprehensive people presence management solution such as WhosOnLocation is a cost-effective and end-to-end solution for addressing cyber security risk that are caused by malicious insiders, both employees and visitors. All visitors are screened before entering the premises and assigned a visitor´s badge that prevents them from accessing off-limit areas. Alerts can be setup to trigger if certain conditions are met as a result of what data is captured form visitors during the sign-in process. Employee attendance can be captured directly in the app or via data sharing with your access control system.

WhosOnLocation enables organizations of all sizes including manufacturing, corporate, utilities, construction, and ICT, to mitigate the risk of insider threats by providing them with an easy-to-deploy and easy-to-use solution to manage their visitors, employees, and contractors.

References

1. *Kaspersky Lab, "The Financial Impact of IT Security on US Businesses", 2017.* https://go.kaspersky.com/rs/802-IJN-240/images/KasperskyLabReport_Financial_US.pdf
2. *Experian, "Data Breach Industry Forecast", 2015.* http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf
3. *PwC, "Global State of Information Security Survey", 2017* https://www.pwc.com/sg/en/risk-assurance/assets/gsiss/global-state-of-information-security-survey-2017-sg.pdf