



InfoSec versus **IT**

Conflating the Two Could Cost SMBs Millions
from Data Breaches



Although cybersecurity, data security, information technology, and system administration fall under the same umbrella, there is a stark contrast between securing data and managing it ...



The main focus, career experience, and skill sets brought by each of these professionals are different, yet they still work together to build secure and reliable digital assets.

Entrusting IT staff to secure data properly is like asking your CPA to audit their work. Mistakes can happen and often get overlooked, and it's unlikely that they will be properly reported. Any errors could cost small businesses millions in legal fees, forensics, brand reputation damage, and customer settlements from a data breach. For this reason, businesses must keep IT staff for maintenance and a dedicated InfoSec team for security.

cybersecurity landscape, the threats that could turn into serious compromise, and the standards and best practices to protect from these risks, which is why data breaches and cyberattacks continue to plague SMBs and cost them millions in damages.

When small business (SMB) owners reference anything under the IT umbrella, they typically think of system administrators, network and server administration, and any staff member who keeps digital assets available and running smoothly. These staff members are critical to the everyday

What's the Difference between InfoSec (Information Security) and IT (Information Technology)?

Before getting into the potential issues from conflating IT and InfoSec, it's important first to understand the difference between the two professionals and their respective responsibilities. It's not uncommon for small business owners to think that an IT staff person, good at system administration is also educated and experienced with InfoSec. Many system administrators are unfamiliar with the

operations of digital resources and network communication. They ensure that users can stay productive and have access to network resources critical to their job functions.

Cybersecurity and **InfoSec** professionals have a very different responsibility.

continued...



“Cybersecurity and IT professionals have a very different responsibility.”

The security of data and the resources that store it are an InfoSec professional's primary concern. IT staff unfamiliar with cyber-criminals' behavior and habits are incapable of identifying threats and could potentially add unknown risks to an organization. InfoSec staff also help monitor digital assets to quickly detect an ongoing attack and contain it in the shortest timeframe and most efficient way possible.

The underground cyber-criminal landscape is always evolving, with attackers finding new ways to scan and exploit vulnerabilities. InfoSec professionals must stay up-to-date with the latest threats and vulnerabilities, and then alert IT staff about the necessity to schedule an update to patch the vulnerable system. This responsibility will save organizations millions from falling victim to unknown threats, and many IT staff do not have the resources to stay familiar with the newest threat actors. InfoSec works directly with administrators to keep systems protected from the latest threats often publicized in advisories available to businesses and hackers.

Although both InfoSec and IT staff have different functions, they still must work together to provide services to a business. Their job functions fall under the same umbrella, so both departments have overlapping responsibilities. For instance, an InfoSec staff member auditing network

infrastructure might find that the network is not properly segmented to protect the billing department data in-motion from other departments located on the same network segment. InfoSec staff would work directly with system administrators to design additional firewall infrastructure to ensure limited downtime and a smooth transition to new network architecture for all users and connected applications.

Network administrators and IT staff responsible for building a secure environment can also be overworked when they have limited knowledge of InfoSec. This issue leads to mistakes, including misconfigurations, missed unpatched vulnerable resources, privilege accumulation and escalation, and unnoticed ongoing attacks from malware and phished stolen credentials. Essentially, cybersecurity and data protection is a full-time job that should have a professional's focus instead of leaving it as an additional workload for an already full-time employee.

InfoSec professionals also work with developers to find vulnerabilities in code. Before developers deploy an application, a code review and scan of services ensures that internal applications are also secure from data disclosure and bugs that could allow anything from malware injection to remote control of a web server.



Just One Mistake Can Cost an SMB Millions and Permanently Damage Brand Reputation

The 2010s brought us some of the most significant data breaches from many cybersecurity blunders, from phishing to ransomware to unpatched public-facing web servers. Some of the decade's biggest data breaches were due to poorly configured cybersecurity, which could have been avoided had the business invested more in InfoSec. Human error is responsible for 30% of data breaches. There are numerous examples from the 2010s to show the dangers of human errors, but a distinct few stand out among the others.

The Equifax data breach disclosed personal data of over 147 million Americans. The vulnerability that cost the organization \$700 million in settlements came down to a simple unpatched web server. The Apache Struts bug was publicly announced and a patch available in March 2017, but Equifax failed to update the critical server software until September 2017. It took Equifax administrators four months to detect the breach, and by then, attackers had already exfiltrated massive amounts of data.

Unpatched systems weren't Equifax's only cybersecurity faux pas. The administrator password to a public-facing web portal was set to the default "admin" value. Due to Equifax's numerous cybersecurity blunders, US government reports admonished the organization for causing one of the biggest data breaches that could have been avoidable. It was also noted that Equifax failed to notice suspicious traffic due to disabled monitoring software with an expired security certificate. In June 2017, administrators updated the security certificate and immediately noticed suspicious traffic.

Every year, Verizon publishes their Data Breach Investigations Report (DBIR), where they analyze over 40,000 cybersecurity incidents and categorize them so that organizations can stay informed of the latest threats.

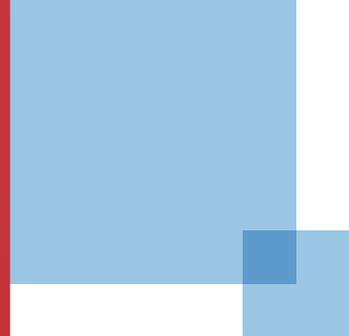
Findings from Verizon indicate that organizations struggle to identify ongoing attacks and contain them quickly. After a successful attack, time is of the essence. The longer an

attacker persists on the network, the more data that can be exfiltrated. Some attackers will slowly exfiltrate data to avoid detection, and it takes organizations months to detect them.

According to the latest Verizon report, it takes only minutes for a compromise and even less time for an attacker to exfiltrate data. The report's concerning trend was that it takes months for an organization to discover the compromise and then days to weeks for administrators to contain it. This means that attackers typically have months to slowly exfiltrate data, leave backdoors open in case of discovery, and possibly add malware to the network threatening data integrity and privacy.

Even the best network administrator can make mistakes, leaving a myriad of cybersecurity issues open to threats. In 2019, a simple DNS misconfiguration left GE Aviation's source code and cleartext passwords open to the public Internet. These misconfigurations can often be caught when the organization combines a team of system administrators to configure and maintain the environment with a type of audit control utilizing an InfoSec team to double-check for errors. This doesn't mean system administrators are incompetent, but rather an InfoSec team combined with system administrators can support each other to ensure each asset's integrity and performance and data protection from potential risks and threats unknown to administrators.

Research from IBM and Ponemon indicate that employee misconfigurations are just the tip of the iceberg. In their Cost of a Data Breach report, malicious and criminal intent were more commonly found to be primary motivation in the latest cybersecurity incidents. This motivation was driven by the financial benefits of exfiltrating private data and selling it to either a competitor or on darknet markets. Malicious and criminal intent was 51% of cyber incidents reported in 2019. Each incident costs organizations an average of \$3.92 million per incident.



SMBs often think that they are not on an attacker's radar because of their small size and limited data stored. This misconception has led to SMBs being a major target for attackers. Recent research polling 500 senior decision-makers at SMBs showed that 60% have no cyberattack prevention plan, only 9% believe cybersecurity should be a top priority, and only 7% of SMB CEOs believed that a cyberattack was probable. 66% of leaders polled believed that a cyberattack was unlikely, making SMBs a larger target than an organization with a cybersecurity strategy.

With the above numbers in mind, Cisco polled 1816 mid-market organizations with less than 250 employees and collected additional concerning statistics. Cisco's research indicated that 53% of small businesses experienced a data breach and these incidents cost 20% of companies \$1 million to \$2.5 million. For a small company, the aftermath and costs of a data breach could potentially put them out of business. Only a third of the businesses polled indicated that they could stay profitable for more than three months after a breach.

From Cisco's research, it's clear that a data breach can put an SMB out of business. By ignoring threats and the need for InfoSec, an SMB's future can be destroyed from a single cyber incident's residual effects. Several other issues resulting in downtime, legal costs, and brand damage linger for potentially years after containment. Cisco reported that 40% of SMBs suffered from over eight hours of downtime. Larger organizations have incident response teams and resilience against downtime (e.g., fail-over resources and quick switch-over to data centers). For an SMB, a day of downtime can be devastating to productivity and profitability.

Even after downtime is resolved, system damage could persist. 39% of SMBs said that system damage added to costs after discovery and containment of an incident. Targeted attacks against an SMB could lead to stolen credentials (e.g., from phishing or social engineering), ransomware that makes it impossible to recover data without paying the ransom, denial-of-service affecting future uptime for the business, and malware installed on the network leaving backdoors for additional attacks.



SMB Challenges with Cybersecurity and Data Protection

Even if an SMB recognizes the need for an InfoSec, there are still major challenges to move from a poorly defended organization to one that takes cybersecurity as an essential factor in day-to-day system administration. It usually takes a professional to bring any business in line with what is considered cybersecurity best practices. Users within an organization are often implicitly trusted, and this is one major mistake that can lead to several types of cyber incidents such as malware installation, ransomware, data eavesdropping, exfiltration, and stolen credentials. Poorly secured environments are vulnerable to numerous threats, but a few are a major concern and introduce higher risks.

A newer threat introduced with the popularity of cryptocurrency is crypto-mining. Cryptomining applications use computer resources to perform calculations, which will generate cryptocurrency for the user when performed faster than other miners. As cryptocurrency became more popular in the last decade, more users began using business resources to mine cryptocurrency. This insider threat has become an issue for organizations that leave open permissions to company resources for any user. With the wrong configuration, trusted users can leave critical assets open to the public Internet.

As counterintuitive as it sounds, organizations need to adopt a zero-trust approach to network security and assume every user could be an attacker, either maliciously or naïve to phishing and social engineering. The zero-trust approach takes most system administrators and users time to get used to, but with InfoSec professionals' help, it can be a smooth transition.

In SMBs, it's not uncommon to give several users full permissions across all systems. As users move to different jobs within the organization, more privileges are added without reevaluating existing permissions. Accumulated privileges are a major issue for SMBs when phishing and social engineering attacks occur. The more users with escalated privileges, the more likely the SMB will suffer from a successful large data breach due to phishing or social engineering.

Of all concerns, an SMB's primary one is often cost. Advanced technology requires the budget to purchase the right architecture and the staff to manage it. Current system administrators also need training to manage new

technology, which adds to costs. Many advanced critical systems can be deployed in the cloud, but this adds complicated risks that only an InfoSec professional can identify.

For example, it's not uncommon for SMBs to outsource storage resources to Amazon Web Services (AWS) S3 buckets. These "buckets" are similar to adding drive storage to the local network and cost a fraction compared to hosting local storage within the organization's infrastructure. Configured S3 buckets become available to users as if they are connecting to local network storage. Forbes reported in 2019 that 39% of error-related data breaches involved misconfigurations. Several major companies left critical documents and data open to the public Internet on these S3 buckets. FedEx left 119,000 documents including passports and drivers licenses open to the Internet. Dow Jones & Company left private data open for 2.2 million customers. Verizon's misconfigured S3 bucket left 100GB of trade secrets open to the Internet. The US government was even responsible for a data leak of government job seekers with classified clearance due to a misconfigured S3 bucket.

“The more users with escalated privileges, the more likely the SMB will suffer from a successful large data breach due to phishing or social engineering.”



“The goal for all parties involved is to improve the organization's cybersecurity posture.”

Leveraging an MSSP to Navigate Murky Cybersecurity Waters

Risk assessment and building the right cybersecurity infrastructure takes a bottom to top approach. Without the right person, the organization needs a professional to assess risk, identify the right integration resources, add the right management tools, and work with system administrators to design a deployment plan that limits the amount of downtime so that productivity is not affected.

For budget conscientious SMBs with limited IT resources, a Managed Security Service Provider (MSSP) is the best solution. Before searching for an MSSP, it's important to understand the difference between an MSP (Managed Service Provider) and an MSSP. The first and primary difference is that an MSSP focuses on InfoSec, which falls under the same umbrella as IT but focuses on data

security and monitoring rather than management and infrastructure maintenance. An MSSP does not replace existing IT staff. Instead, an MSSP works directly with IT staff to ensure data security and reduce existing risk to ongoing and future threats.

The goal for all parties involved is to improve the organization's cybersecurity posture. This requires a number of steps that can take several months to complete. An additional consideration is the SMB's industry and any regulations surrounding data security. HIPAA, DFARS, PCI-DSS, SOX, GDPR and FedRamp are just a few regulatory standards that must be incorporated into InfoSec architecture. An MSSP will be aware of these regulations and provide advice accordingly.

IBM's Cost of a Data Breach report highlights cost benefits with adding InfoSec to the network environment. The biggest savings were in forming an incident response team, use of encryption and having incident response tests and planning. The reason incident response has such a large impact on cost savings is because the right team can detect and contain an ongoing attack quickly, which minimizes the amount of stolen data stolen as an attacker is unable to spend months accessing internal network resources.

The use of IoT, mobile, and cloud infrastructure have an inverse impact and increase risk. This is largely due to companies offering to bring your own device (BYOD) to give more flexibility to employees who work remotely. These three factors increase risk due to device theft, misconfigurations, and an increased attack surface. Companies face the problem of BYOD risks while still providing the flexibility that mobile and IoT offer.

A competent MSSP can handle many of the other challenges related to InfoSec. The use of basic encryption has cost-savings benefits, but for an organization unfamiliar with the proper ways to implement it, deploying the wrong encryption strategies can be useless and give a false sense of security.

Before choosing a provider, it's important to understand what an MSSP can offer versus an MSP. An MSSP can either bring an organization with poor security to current standards or improve existing infrastructure to ensure better data security.

George Makaye, CISSP



ABOUT

George Makaye, CISSP
CEO and Founder, Makaye InfoSec



As CEO of Makaye InfoSec, George Makaye, CISSP, helps businesses, local governments, and nonprofits protect private information and data.

When you hire Makaye InfoSec, you get a true cybersecurity partner. We are committed to helping you reach business goals, protect your community, and carry out your mission. We believe that it's just not right that cybercriminals target organizations that are trying to do good in the world, which is why we provide the support you need to make cybersecurity choices that help you succeed.

Contact Information:
Email: smla@minfosec.com
Phone: (972) 645-2231
LinkedIn: www.linkedin.com/in/georgemakaye
Address: 269 Renner Pkwy Ste 200
Richardson, Texas 75080