The MSSP: Dedicated Cybersecurity Support That Every Corporate IT Team Needs

Because You're Fighting On More Fronts Than You Can Handle

No IT team can simultaneously fight on every front in the cybersecurity war

IT and cybersecurity professionals are a lot like modern military leaders deployed to conflicts around the globe. They face highly motivated adversaries across multiple battlefronts who often employ non-conventional tactics, all while under the watchful eyes of the U.N. and other international regulatory organizations.

Just like combat leaders, today's IT and cyber-security professional manages a 360-degree battlefield with omnipresent threats and regulatory infringements looming at all times from every direction.

"Nearly half of all enterprises were hacked in the last 12 months. More troubling, among these businesses, the average suffered 29 hacks."
— TechRepublic

Saalex
Information Technology
The IT Experts

AS A CYBERSECURITY DEFENDER

You are never fighting just one type of battle at a time

Perhaps you have never thought of your role this way, but you lead a team in a high-stakes struggle to control and dominate the cyber battlespace. Whether you are a CISO, chief privacy officer, director of IT or other IT professional responsible for your firm's cyber defenses, you are fighting a multi-front war every day for the digital security and integrity of your company.

Your primary adversaries in this war are cybercriminals. Between 2017 and 2018 alone, this group attempted to hack nearly half of all enterprises.[1] But hackers are not the only threat — consider a few of the following battles you will also need to fight while simultaneously countering the cybercriminals:

Human error — inadequate cybersecurity training and lack of email security tools could be a problem at your company through Business Email Compromise (BEC)

Rogue and disgruntled employees

Lack of cybersecurity expertise in areas of vulnerability scanning, penetration testing and compliance controls and policies

Difficulty keeping track of where your sensitive and proprietary data resides

Struggles to secure a sufficient cybersecurity budget, putting your IT team at a disadvantage in all of these other battles

Growing and changing regulations and laws

To fight so many cyber-battles simultaneously, corporate IT teams need expert help.

Just like a platoon leader calling in air support when outnumbered, your IT team needs skilled, experienced support to help you with the multiple battles in your ongoing cybersecurity fight.

This paper will review in more detail the various cybersecurity challenges we alluded to above — all of which your team will need to address simultaneously — on your road to mission success.

Next, we'll explain why data security and data-security compliance are two separate issues requiring different expertise, and why this makes being your company's cyber-defender even more complicated. However, it is not a mission you have to take on without reinforcements.

Finally, we'll discuss why it makes sense to outsource many of these complex cybersecurity initiatives to a trusted third-party expert — specifically a Managed Security Service Provider or MSSP.

CORPORATE CYBERSECURITY PROTECTION: *ONE GOAL, MANY THREATS*

Let's look more closely at some of the major battles your IT team must fight in your ongoing campaign to protect your company's networks, sensitive data and other digital assets.

1 Lack of an overall cyber risk management strategy

According to a November 2018 feature in CSO Magazine

"The ramifications of poor cyber risk management practices carry a high cost."[1][2]

The article points out the following ways that defending an organization's cyber infrastructure and digital assets has become more complex and difficult than ever:

- The enterprise's *"attack surface"* keeps growing (i.e., there are more devices, apps and networks to protect), and this creates more vulnerabilities.
- Threats are growing more sophisticated.
- Businesses now face risk from cyberattacks on multiple fronts, including financial risk, operational risk and reputational *(brand value)* risk.
- All of these realities *(threats, the hackers themselves and your company's cyber-infrastructure)* are changing constantly, and all aspects of cyber risk management are interrelated. When any of these things change, it affects everything else.

2 Cybercriminals

Unfortunately, the global community of cyber bad actors grows both more sophisticated and brazen every year.

They have hacked Yahoo!, Equifax, Target, Facebook, Capital One, LinkedIn, Sony and millions of other businesses. Because stealing corporate data has become so lucrative, the numbers of hackers grows each year as well. The following are just a few examples of why you need to consider cybercriminals a continuous top-priority threat to your business:

- Experts estimate that almost 60 percent of all companies have experienced at least one cyberattack *(e.g., DDoS, phishing, social engineering hacks)*.[2]
- Research cited by IBM found that in 2019 the average total cost to a business suffering a data breach was nearly $4 million.[3]
- As concerning as these stats are, they will likely only to get worse with time. According to a 2018 industry study, cybercriminals are expected to steal 33 billion records in 2023.[4]

Given the increasingly sophisticated and creative methods hackers are finding to penetrate even the most advanced corporate security perimeters, you cannot expect your in-house team to be ready at all times for every potential type of attack.

3 Human error

Even if your team were able to build an IT environment that no hacker could directly pierce, *(which is not possible, just to be clear)*, you would still face a different type of cybersecurity risk — innocent employee mistakes that let hackers walk right through your digital front door.

As a 2018 article in *CSO Magazine* reported, 92 percent of malware is still delivered by email.[5] This means millions of employees are still naively opening messages in their corporate email from unfamiliar addresses or senders pretending to be trusted colleagues or vendors.

Many employees are clearly also taking whatever actions these malicious senders ask them to by opening attachments, clicking links or visiting websites referenced in the emails. Cybercriminals use these methods to launch ransomware attacks, steal files or otherwise create digital mischief for these employees' companies.

9 in 10

Data breaches are due to human error

According to data reported in TechRadar.[6]

This explains another statistic cited in the same CSO article: More than half of IT decision-makers say phishing scams are their top security concern.

As if that were not enough to worry about, there is another category of human error that is responsible for a significant percentage of corporate breaches — misconfiguration of servers and systems.

A 2018 IBM Security study found that 43% of all corporate records compiled that year *(990 million!)* were exposed due to misconfigured cloud storage systems and databases.[7]

That same IBM report also found that misconfiguration is now the single greatest threat to cloud security, and 62 percent of IT security professionals say it's a problem in their companies.

Addressing the ongoing threats of human error — including innocent IT mistakes made setting up your cloud data infrastructure — requires more than reminder emails warning your staff about the dangers of cybercrime.

It will require a systematic approach that includes employee training, periodic readiness tests and ensuring your own IT personnel have the knowledge to secure your data effectively, whether on-premises or in the cloud.

In other words, this is another front altogether in your larger cybersecurity war, and it requires the help of subject-matter experts.

4 Malicious insiders

Yet another battle your IT team needs to ready for is the threat from a malicious insider — an employee or consultant who has legitimate access to your network but who uses that access to steal digital assets or create other problems for your organization.

As US Cybersecurity Magazine points out, malicious insider attacks can be the most difficult for an organization to prepare for, or even to identify after the fact, for the following reasons:

- Attackers have access to your digital infrastructure and they can move around your network without scrutiny. Employees who commit bad acts against your company *(stealing data, inserting malware)* will have plenty of time to cover up their actions before anyone knows what has happened.
- An angry employee who wants to attack your network can mask their intentions afterward by pretending it was an honest mistake.
- An employee who has just been fired *(or is expecting to be fired)* can slip malware or another type of attack into your network and keep it dormant and hidden until sometime in the future, giving the employee a chance to create havoc on your company anytime they wish.

These are not just hypothetical concerns. A 2018 report from CA Technologies found that more than half of organizations surveyed said they had actually suffered an insider attack during the previous year. In addition, 90 percent of these companies' IT teams said they feel vulnerable to threats from malicious insiders.[8]

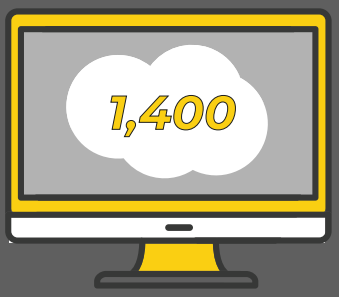
Because it is a different category of digital-security threat that requires another set of skills and expertise, the risk of a malicious insider is another reason to find third-party help with your company's cybersecurity.

5 Runaway data

One of the less-discussed cybersecurity battles is the fact that business data is now growing at such a rapid pace, and employees are generating, storing and accessing this digital information across so many different platforms and devices. Before you can secure your company's proprietary data, your IT team needs to know where it all resides.

Research Reported By McAfee

In 2016 the average enterprise was using more than



different cloud applications

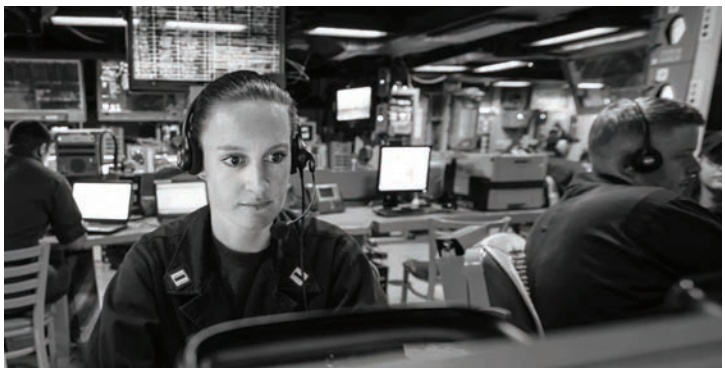
That number tripled between 2013 and 2016, and one can only assume it's even higher now

The report also found the average large business uses 76 different file-sharing apps, and nearly one in five files that employees upload to these cloud services contains sensitive corporate data *(e.g., financial records, personally identifiable information [PII], electronic protected health information [ePHI]).*

Complicating matters further, employees now use multiple devices, both within your offices and outside, to generate and access company data. A Microsoft study found that two thirds of employees use their personal mobile devices for work, even in organizations that prohibit doing so.[10]

A 2018 Google-commissioned study by Forrester Research found that more than half of cloud-based workers said they like to switch between devices to get their work done.[11]

Given you're responsible for protecting more data than businesses have generated at any time in history, and that this data is spread across so many devices — including many outside your corporate firewall — you need to consider this another ongoing digital security threat. If an employee's personal smartphone can access your corporate network, then that smartphone is part of your cybersecurity war, and there is a good chance your IT team isn't treating it as such.



Knowing how to bring all of your sensitive and regulated data under your corporate protection, wherever it resides, represents yet another battle in this war, requiring yet another type of domain expertise.

Keep in mind, this article is pointing out the risks of having a poor cyber-risk management strategy. You can imagine how much more dangerous it would be to have no such plan in place.

New ESG research underscores the growing need for third-party cyber risk management — even extending to all of an organization's business partners.

The final challenge we're going to discuss is bringing your IT security practices into compliance with your industry's regulations.

To be fair, the lawmakers and industry enforcers are trying to help when they insist you follow specific rules to protect your data — HIPAA for health providers, the ABA for law firms and NIST for federal agencies and contractors. However, because complying with these rules can be a challenge in and of itself, and because failure to do so can lead to steep penalties, it's also fair to think of regulatory compliance as a separate battle in your company's cybersecurity war.

In other words, despite regulators' good intentions, the weapons they devise to thwart hackers can also affect your company.

One way to understand your organization's risk from regulators is to think of it as friendly fire.

Imagine a platoon leader who discovers a large enemy encampment mid-march. There's no way to maneuver around the enemy and still have time to complete the mission, so the team will have to go through that encampment.

The enemy clearly has the numbers, so the platoon leader decides to call in close air support. That leader had better know precisely which coordinates to send those airships, and had better make sure the entire platoon is at a safe distance from that zone, or else their own team overhead might accidentally hurt them.

Your industry's regulators may have devised data-protection guidelines or laws to help your organization protect itself against real dangers: hackers, human error, natural disasters and so on.

Regardless of those regulators' motives, if your company fails to comply with the strict letter of their laws, they could end up hurting your business.

Here are just a few examples

- If HIPAA regulators determine a health organization has failed to safeguard its patients' electronic health records, the fines can range from $10,000 to $50,000 per record, up to $1.5 million per year for each violation.[13]

- Financial institutions that fail to secure consumer's private financial data to the satisfaction of the federal Gramm-Leach-Bliley Act (GLBA) can face penalties of $5,500 to $1.1 million per record.[13]

- For businesses that want to do business with the Department of Defense *(or sub-contract for department contractors)*, compliance with DFARS/NIST 800-171 will soon be mandatory and require an audit from regulators. Failure to meet these standards will prevent your business from even being able to bid on contracts.

Complying with your industry's regulations is a full-time job

To give you an idea of how challenging and time-consuming it is for any in-house IT team to keep their organization compliant with their industry's relevant data-security regulations, let's review some basic details about these regulations.

The NIST self-assessment handbook for cybersecurity has more than 150 pages.[14] *(Written mostly in legal jargon, it is not an easy read.)*

The rulebook for the financial industry's self-regulating body, FINRA, is more than 1,300 pages. Like the NIST manual, it is also written in dense legalese, including hundreds of clauses like this one:

For purposes of paragraph (b)(3) of this Rule, the following are the covered functions:

> **... (n) defining and approving business security requirements and policies for information technology, including, but not limited to, systems and data, in connection with the covered functions.**

The HIPAA law is so dense and complex that the Department of Health & Human Services' "HIPAA Administrative Simplification" manual is itself more than 100 pages *(again, all in legalese)*.[16]

DATA SECURITY AND DATA-SECURITY COMPLIANCE ARE TWO SEPARATE INITIATIVES

Contemplate the following as you consider the massive amount of work required to bring your company's entire IT infrastructure into compliance with HIPAA, the ABA, FINRA, GLBA, Sarbanes-Oxley (SOX), DFARS/NIST, the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and others.

Achieving full compliance with your industry's regulators does not necessarily mean your organization is protected against all cyber threats.

Nor does implementing the most advanced cybersecurity infrastructure mean you are in full compliance with any of these regulations.

Data security and data-security compliance are not the same thing. They both need to be undertaken as separate objectives, and each will require different knowledge and expertise.

Are you compliant today?

For a sense of where your company stands today in terms of data-security compliance, here are a few self-assessment questions:

- Does your company have a written incident response plan ready to show an auditor right now? One of NIST's requirements is that organizations have a documented plan to deal with cybersecurity incidents.

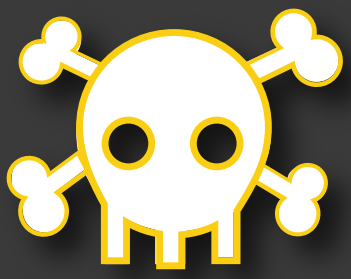
- Do you conduct periodic stress tests of your data backup systems and document the results? FINRA compliance requires regular backup-integrity testing for consumers' personal financial data.

- Do you have a written termination procedure in place? Among the administrative safeguards required by HIPAA, organizations must have a documented procedure that ends an employees' access to all networks and digital assets upon termination.

- If a NIST regulator audited your company today, would you have this detailed documentation ready? One of the framework's "Security Assessment" rules is that organizations:

  "Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems." (NIST 180-171, Section 3.12.4.)

If you would like a detailed self-assessment for any of these (or other) data-security regulations, contact a SaalexIT solution architect.



THE CYBERATTACK THREAT: IT'S A MATTER OF WHEN, NOT IF

In the field, a combat platoon leader has to act as if contact with the enemy is inevitable. They keep their team's readiness at the highest level, leveraging the latest tech while maintaining full awareness of the rules of engagement.

A cybersecurity team operates in a similar environment when countering threats that target your organization every day.

Given the growing prevalence of cybercrimes, the increasing sophistication of hackers and the ever-expanding regulatory demands on businesses like yours, you need to prepare for an inevitable cyber emergency. It could come as a hack from an outsider, an attack by a malicious insider or even an audit by industry regulators. Assume that you will eventually face one of these situations at some time.

When you do, you'll need help.

The MSSP: Your most effective, affordable solution to cybersecurity challenges

We've discussed a wide range of initiatives in this paper: fortifying your cyber defenses, training your employees to become more hacker-savvy and street smart, identifying the hundreds or even thousands of locations where your corporate data resides so you can secure it and bringing your IT environment into compliance with your industry's regulatory standards.

Rather than trying to develop this wide-ranging knowledge base internally while deploying your existing IT team to manage these tasks, it makes sense to outsource these initiatives to a business focused exclusively on every aspect of corporate cybersecurity.

Here is a small sample of what the right Managed Security Service Provider (MSSP) can do for you:

- Vulnerability Management
- Threat Intelligence
- Incident Response
- Intrusion Detection
- Cloud and On-Premises Protection
- Managed Detection and Response
- Cloud/Security Orchestration & CASB
- 24x7x365 Monitoring
- 24x7x365 Help Desk
- Regulatory Assessment and Compliance *(NIST, HIPAA, ABA, FINRA, SOX, GLBA, GDPR, etc.)*
- Backups and Disaster Recovery
- Quarterly Business Reviews *(VCIO)*
- Email Encryption/Spam Filtering/Imposter Prevention
- Web Content Filtering
- Antivirus/Anti-malware
- Infrastructure & Device Management
- Firewall Management
- Identity and Asset Management
- Security Information Event Mgt. & Logging *(SIEM)* and SOC-as-a-Service
- Disk Encryption/Protection
- Multi-factor Authentication
- Vulnerability Scanning
- Security Awareness Testing, Training
- Endpoint Detection & Response *(EDR)*
- Intrusion Detection System *(IDS)*
- Incident Threat Response *(ITR)*
- Data Loss Prevention
- Network Access Control
- Change Monitoring
- Web Application Firewall

For an evaluation of your company's cybersecurity readiness, contact a Saalex IT solution architect.

References

1. TechRepublic: Nearly half of all enterprises were hacked in the last 12 months

2. *CPO Magazine*: 11 eye-opening cyber security stats for 2019

3. IBM Report: The 2019 cost of a data breach

4. Norton: 10 cyber security facts for 2018

5. *CSO Magazine*: Top cybersecurity facts, figures, and statistics for 2018

6. TechRadar: 90 percent of data breaches are caused by human error

7. IBM Security: X-Force Threat Intelligence Report Index, 2019

8. CA Technologies: Insider Threat Report, 2018

9. McAfee: 12 must-know stats on cloud usage in the enterprise

10. CBS News: BYOD alert: confidential data on personal devices

11. Forrester Report: Rethink Tech in the Age of the Cloud Worker (commissioned by Google)

12. *CSO Magazine*: It's Time for a New Cyber Risk Management Model

13. Compliancy Group: HIPAA Fines

14. Faruki Law, PLL: Privacy Law Basics for GLBA

15. NIST.gov: NIST MEP Cybersecurity Self-Assessment Handbook

16. FINRA.org: FINRA Rules

17. HHS.gov: HIPAA Administrative Simplification, Regulation Text