Identifying the *real* security threats to your business

Develop the correct risk posture to protect your data – *and* your company

By Michael DaGrossa, CISSP, CEH, CCE
Vice President, Business Risk Services, Essextec

March 2014

White Paper

essextec
GETTING IT DONE TOGETHER

INTRODUCTION

Alligator attacks make good headlines — and when you live in the Florida Everglades, alligators may be a real threat. For the rest of us, we see the headlines, but know we don't necessarily need to worry about alligators. It's the same story with security risks: while some types of attacks may grab headlines if you run a small or mid-sized company, they're probably not *your* biggest source of risk.

With the constant barrage of information, the scarier and louder something is, the more attention it gets. I propose that we address today's security risks with common sense: understand what can bite, what can bite *you*, and how to prepare for an attack.

WHERE IS THE REAL DANGER?

For a global view of the risks to your security, we consider several different categories of threats:

Inadvertent Threat Actors (ITAs)

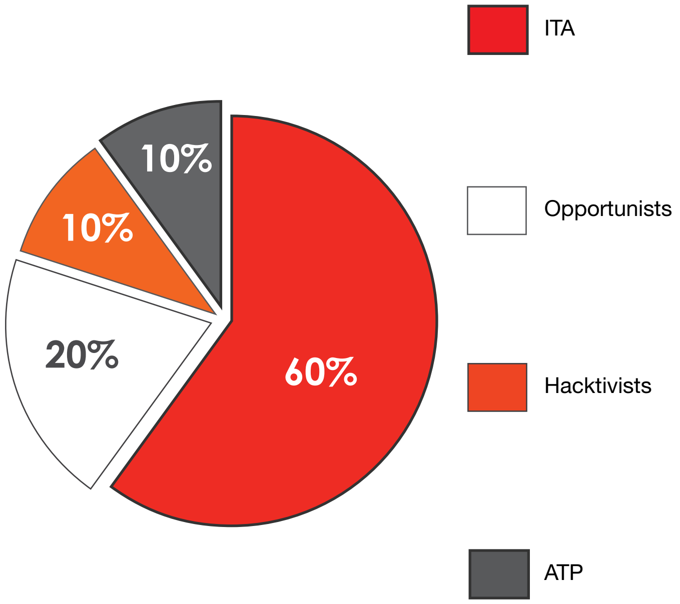
Recent studies from IBM show the *real* persistent threat most clients face is from the inadvertent actor. ITAs are insiders — employees, contractors, outsourcers — and they constitute 60 percent of attributable security incidents. These are not experienced hackers — they cause harm inadvertently (accidentally) by unwittingly carrying viruses or posting, sending, or losing sensitive data. Alternative attack vectors are becoming more and more commonplace, including targeted emails with malicious attachments that appear to pertain specifically to you or to your professional industry (spear phishing attacks), social engineering attacks over the phone or in person, or mobile device-based malware. The possibility of being attacked by an ITA has never been higher.

Opportunists

These are generally "script kiddies" (bored types with very little experience, but with the ability to follow directions and to run basic tools) who are creating worms and viruses. They make up 20 percent of attributable security incidents. Like ITAs, opportunists tend to be inexperienced with limited funding. They target known vulnerabilities using viruses, worms, Trojans, and bots. They act mainly for thrills and bragging rights. With the proper tools, these types of threats are easily detected.

Hacktivists

These are White Hat and Black Hat hackers — self-described protectors of freedoms or some other seemingly worthy cause. They make up less than 10 percent of attributable security incidents. Their profiles range from inexperienced to higher-ordered skills. They target known vulnerabilities in a system. While hacktivists tend to prefer denial of service, they often use malware to introduce more sophisticated tools and escalate privilege. Hacktivists are detectable, but hard to lock down and hold accountable, mainly because of the mesh network which could be vast, *i.e.,* Anonymous, but organized.



Threat Category Percentages

Advanced Persistent Threat (APT)

The final category — and the most damaging — is the Advanced Persistent Threat (APT). These threats tend to come from national governments, organized crime, industrial spies, and terrorist cells. Although they make up less than 10 percent of the attributable incidents, they are the ones that grab the headlines. Typically based in foreign intelligence or other organized crime, APTs possess sophisticated skills and are well financed. In fact, they often act for profit. These attacks are carefully planned and strategically focused. They target technology and information that have a high value. APTs establish a covert presence on sensitive networks and are very difficult to detect. They are also increasing in prevelance.

Most industries disproportionately worry about APTs. They are headline grabbers and a real threat for some larger companies. Unfortunately, most businesses find the idea of securing their data from this type of attack to be too daunting and too costly. Others think that the likelihood of being targeted by a foreign government is very low, so they are lulled into a false sense of security, *i.e.,* “That won’t happen to me”.

Although the likelihood of an APT targeting a small to mid-sized company may seem far-fetched, it can and does happen. One simple reason is the theory of constraints: you are only as strong as your weakest link. Many large organizations use third parties for a multitude of reasons. Often, the same internal controls used to protect against the smaller attacks can reduce the likelihood and impact of a larger scale attack, such as an APT. Just as with the alligator example, understanding your risk posture will help to set the appropriate internal controls for your organization.

However, as you can see, the reality is that APTs make up just 10 percent of incidents while, at 60 percent, ITAs are the real threat to most companies. ITAs are often due to members of your own team who are unwittingly used by others with malicious intent who can carry out highly damaging and prolonged attacks without arousing suspicion. More than 70 percent of ITA incidents can be attributed to end-user error and misconfigured systems or applications.

WHAT CAN YOU DO ABOUT IT?

There is no one-size-fits-all solution. Organizations need to understand their individual risks and use that data to make a foundational recommendation for a layered approach to security. What is the likelihood of being targeted by a foreign government? That depends. What is the likelihood of exposure by accidental or inadvertent risk? It’s almost certain.

The focus should be on identifying and controlling the real threats to your business. According to IBM, many of the breaches reported in the last year were a result of poorly applied security fundamentals and policies. These breaches could have been mitigated by putting basic security hygiene into practice.

When you understand how security and risks fit into your environment, you will make your organization less vulnerable and much more efficient. The key is to adopt the proper risk posture. This requires understanding your specific risks and how to mitigate them.

Establishing a risk-aware culture for *your* organization will help guard against getting swayed by media hype and focus your team on your security needs. You’ll put controls in place to help defend against the real risks you’ve identified.

WHO SHOULD BE CONCERNED ABOUT RISK?

In a word: everyone. Data is at the heart of any risk and has intrinsic value, whether it’s customer emails or credit card numbers. We help executives determine the true levels of risk and typically find that each functional area has a different concern:

> CEOs — competitive differentiation
> CFOs — compliance within regulations, laws, or standards
> CIOs or CISOs — securing technologies
> CHROs — labor
> CMOs — protecting the brand
> COOs — protecting the internal workings of the organization

In a risk-aware culture, you have zero tolerance for employees and vendors who are careless about security. This means creating and enforcing policies that limit people in positions of authority from exercising discretion or changing penalties to subjectively fit the circumstances; they would be required to impose a predetermined penalty, regardless of circumstances. This is a cultural change that, if administered properly, can be a business-enabling tool that increases efficiencies while limiting risks. This change needs to start at the top of an organization and be clearly communicated to every level.

Once we identify pain points and threats to each of these areas, we start to quantify actions that can be taken. The goal is to create controls to protect data *and* your organization.

PROTECTING YOURSELF

When it comes to protection, we look at three points in an organization: people, processes, and technology. We use a basic risk principle on these areas by assessing the susceptibility, impact, and risk.

As previously stated, security cannot be a one-size-fits-all approach. Today's threat trends are dynamic, multi-faceted, and range from accidents to targeted, state-sponsored, cyberterrorism. At first, the controls you need may be basic, then eventually become more proficient, and finally develop into fully optimized or mature safeguards.

You need to ensure that the controls you put in place are appropriate, using either manual or automated processes. Using tools to track your progress, adjustments can be made to the risk/security lifecycle, as needed.

The goal is to establish a mature security and intelligence-based approach for your organization moving from reactive, manual processes to proactive, automated ones. Security intelligence lets us see what's actually happening, understand the real threat landscape, and use advanced analytics to develop real insight into the kinds of attacks that you're experiencing — and how to prevent them.

A CLOSER LOOK AT SECURITY INTELLIGENCE

The evolution of Security and Incident Event Management (SIEM) is a good example of the way that a technology tool has changed because of people and processes. This tool started out as log parsing, which was a way to look at information that systems tracked as well as key aspects of those systems (hardware, software, web, etc.). But as systems became larger, so did the data — and log parsing became log correlation. With log correlation, multiple types of logs could be viewed by a single system and, potentially, by a smaller group of people. As the number of events grew from hundreds to thousands to hundreds of thousands, it would take teams of people to view all the data — and those people had to know which patterns to look for.

Enter Security Intelligence (SI). Now these systems have evolved to be able to automatically pick up patterns, signatures, and events that are known to be problematic. With this additional detail, a security administrator can create additional policies that both raise alerts *and* stop activity.

Today's SIEM is actually an SI engine that enables your security workforce to see information that's pertinent to your risk posture. For example, a business analyst can have access to sensitive data as part of their job for a specific set of tasks. Their actions would be logged, but they wouldn't raise an alert. However, if that analyst tries to access the same files from a remote system, foreign network, or at different times of the day (for instance 3:00 a.m.), your system may have automated processes that raise an alert.

This example demonstrates that technology does not evolve in a vacuum — it's affected by people and processes. You can see that SI was affected by data classification, data protection, change/control management, acceptable use, mobile management access controls, role based access, incident response, and even forensics.

The bottom line is that your data must be protected throughout its full lifecycle and that protection must be continually monitored and adjusted.

CONCLUSION

It's critical to understand your risk posture so that appropriate controls can be set for each organization's specific situation and needs.

Essextec's Business Risk Services team can help organizations identify and justify control objectives around people, process, and technology.

ABOUT THE AUTHOR

Michael DaGrossa, CISSP, CEH, CCE
Vice President, Business Risk Services, Essextec

Michael is a recognized expert in the field, with nearly two decades of experience in information security and investigations. Michael's professional experience includes several leadership positions in the medical, public accounting, technology, finance, and pharmaceutical industries. While in the corporate world, he developed and implemented security policies, compliance programs, disaster recovery, business continuity, digital forensics, and technical security assessments. His expertise has allowed him to provide services for high level engagements to industries in multiple sectors.

Michael holds the following certifications:
Licensed Private Investigator; Computer Information Systems Security Professional (CISSP); Certified Computer Examiner (CCE); Certified Ethical Hacking and Countermeasures (CEH); Access Data Forensics Examiner (ACE); IT Infrastructure Library Foundation Class and Certification (ITIL); LeaderShift; Internal AIG Leader Training; Microsoft Certified Systems Engineer (MCSE); Microsoft Certified Trainer (MCT); Citrix Certified Administrator (CCA); Cisco Certified Network Associate (CCNA); Novell 4.11 Certified NetWare Engineer (Expired); and Certified Technical Trainer - Train the Trainer Program, Department of Homeland Security.

Premier Business Partner IBM

essextec
GETTING IT DONE TOGETHER

Dynamic Infrastructure I Data Management / Analytics I Business Risk Services
www.essextec.com