INSTITUTE FOR ROBOTIC PROCESS AUTOMATION & ARTIFICIAL INTELLIGENCE

The Five Greatest Cybersecurity Challenges Plaguing SMEs

Jim Noble
CEO
Integrated Cyber Solutions

I recently got together with a group of like-minded people. Some of them have managed cybersecurity services companies. Some have Certified Information Systems Security Professional(CISSP) qualifications. Some have been watching this industry for the past 20 years.

We all had one thing in common: a troubling realization that the industry has spent a fortune trying to keep bad actors out (with some degree of success) but has failed time and time again when it comes to keeping out sophisticated attackers.

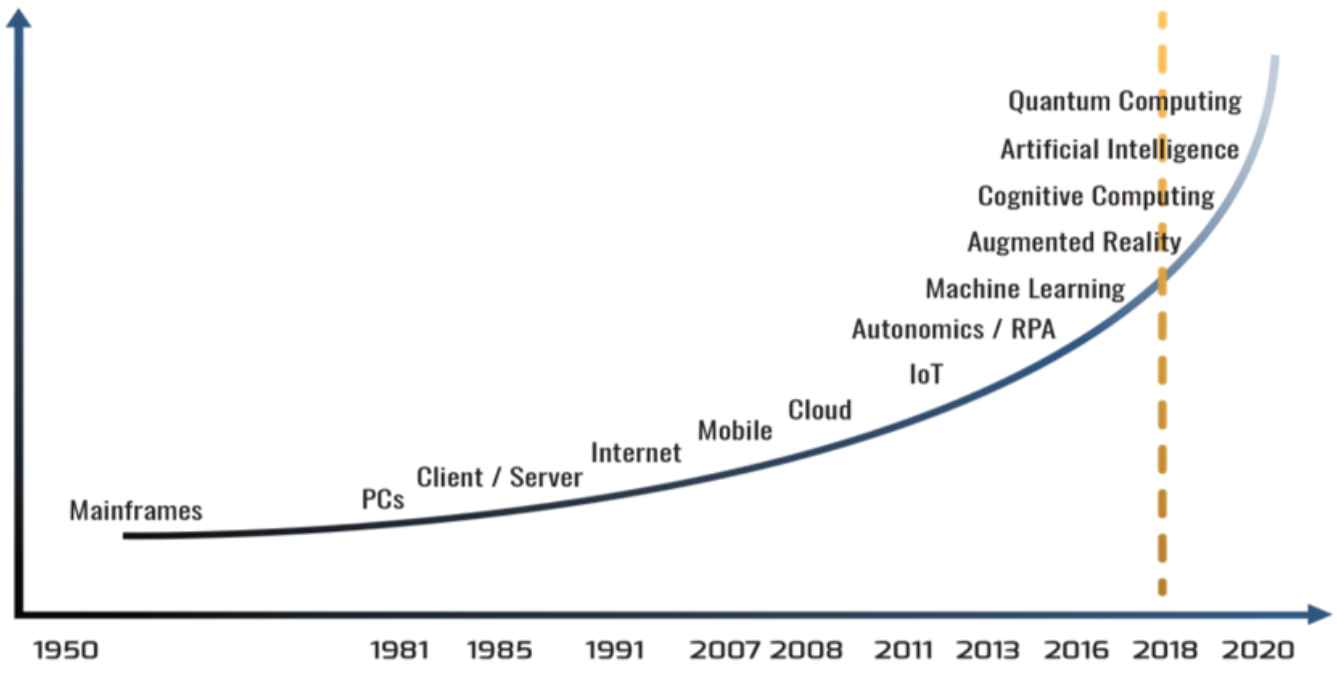
This is the primary challenge that everyone in the world of cybersecurity faces today.

There is one main reason so many industry professionals are behind the times: The pace of change is accelerating exponentially. Every day, the challenges grown more daunting.

With the advent of artificial intelligence (AI), machine learning, augmented reality, cognitive computing, and other technological advances, attackers have an entire arsenal of tools at their disposal. The predators are moving faster than their prey. It has taken us, the defenders, everything we have to just keep up.

Being an attacker is easy. They know how to find shared tools, including stolen NSA assets, on the dark web. They have the element of surprise on their side. And they don't even have to get out of bed! Best of all — if you're a malicious actor, that is — they rarely get caught and make tons of money without investing much.

Against such odds, it is no wonder that even seemingly vigilant companies may never see them coming — even after the exploit begins. And when it comes to small and medium-sized enterprises (SMEs), the deck is really stacked against you.



Problem #1: Keeping Up with Complexity

If you're on the side that is trying to prevent an attack, you have probably deployed a wide array of tools and software solutions. The following represent just a few of the most common cybersecurity practices:

- You maintain an antivirus solution
- You employ an identity and access management (IDAM) solution
- You employ a network access control (NAC) solution
- You may employ encryption and decryption and data loss prevention (DLP).
- You may allow Bring Your Own Device (BYOD) among your staff and, if you do, you probably employ mobile device management
- You surely block suspicious URLs through a blacklist
- You quarantine specific incoming files and exorcise them

Beyond all the usual defense strategies, I hope you have a good architect crafting your key point solutions. I hope you have strong processes in place to keep all of these point solutions current.

I could go on and on about the cybersecurity best practices, processes, and capabilities that we all have in our defensive playbook. But the point I am trying to make is that the challenges of this profession are daunting, and most companies simply cannot keep up.

Challenge #2: Keeping Up with Workload

One of our clients has about 500 employees. Even for a company of this size, the workload can be staggering. To drill down into the scope of the problem, we need to realize that a networking device like a firewall, wireless access point, or router typically generates about 20 events per second (EPS). This means a firm of this size has around 400 EPS.

Then you have the infrastructure servers (such as domain controllers, active directory, and proxy servers), Windows servers, Linux servers, and virtual machines in the cloud. These have fewer events per unit, but they add up quickly. And then, of course, most companies also have the endpoints like desktops, laptops, tablets, and smartphones. Overall, these devices usually account for about half the EPS.

Combined, you are talking about 1,000 events per second — or more. Let's do the math: 86,400 seconds in the day multiplied by 1,000 events per second, and now we are talking about at least 86,400 million events in a single day. And this isn't even a large company!

Obviously, no team can manually analyze upward of 100 million events in one day, so they rely on solutions including security incident and event management (SIEM) tools. Such software will typically give you a thousand-fold reduction when it comes to classifying events that could potentially indicate a compromise. So, by using the SIEM, the company would likely cut its volume down to about 100,000 flags per day.

Interestingly, this is essentially what was at play during an infamous breach that infected one famous retailer. It was using a perfectly good SIEM, but on Thanksgiving Day — the company's busiest sales day of the year — it received a massive influx of traffic. The cybersecurity team was sinking in a sea of noise.

They couldn't determine what was material and what was not — and this continued for weeks. In fact, it took until Christmas for the retailer to discover the substantial compromise within its point-of-sale (POS) system.

On one hand, the 27 days that passed between the original compromise and the eventual discovery is far better than the industry average of 200 days. But this lagtime still left the company reeling from costs that exceeded $162 million.

Since that incident, new solutions have emerged. IT teams now often use a tool known as SOAR (security orchestration, automation, and response). These SOAR solutions allow you to perform what we refer to as "context fusion," meaning that you are alerted to relevant events arising from multiple sources of threat intelligence or other companies similar to your own. SOAR tools (including popular versions from companies like DarkTrace and DFLabs) help you to reduce the number of flags down to as low as 0.2% of the volume that had been coming out of your SIEM.

Looking back to our example, the 500-person company would now be sending only around 100 events per hour to its security operations team. And since the firm's System and Organization Controls (SOC) is staffed by very clever people, they are capable of solving many standard security incidents. On the face of things, this seems manageable.

The problem, however, is that the bad guys don't sleep at night. They don't take holidays. They don't take breaks. In fact, the bad actors have all these advantages because they're not even people. They are robotic software that work to penetrate networks by crawling IP addresses looking for vulnerabilities.

What does this all mean? In our example, the company would need at least five people in its SOC working in a three-shift system. And these five staff members must cover illnesses, days off, and holidays. That is certainly an expensive proposition.

Problem #3: Focusing on the Wrong Threats

Many chief information security officers (CISOs) and IT security directors are overly focused on compromise prevention and preventing malware execution. While these threats still exist, the real threat has moved on, and many of the old techniques have fallen to the wayside. Conventional wisdom is behind the times. Even the words we use — malware, viruses, Trojan horses, honeypots, and quarantine — are antiquated.

We are now facing a new wave of non-malware threats, including drive-by exploits, sessions established to MS-Powershell, access via open source defects in web utilities like Apache Struts, and a range of other attacks that don't require the bad guys to download any malware because they instead stream the exploits. As far back as 2017, the Ponemon Institute issued a report stating that 53% of known compromises did not involve malware.

On the contrary, a typical scenario may involve a user visiting a website and "mousing" over a location where Flash is loaded. The Flash invokes windows PowerShell, which establishes a session and that session sends sensitive data to the attacker with no executable file ever being downloaded.

So, if our conventional defenses focus on identifying threats that expect a file to be written to disk, how can we be protected against new threats? While preventative measures are still important, IT teams need to focus on one key question: Would you be able to react in real-time in the event of a breach?

After addressing that fundamental concern, consider the following: Do you also monitor the log files from all of your assets to look for unusual activities? Do you do this 7/24/365? And if you do discover something, can you intervene and contain the problem before it propagates?

Think about the WannaCry encryption key. If your company was penetrated through this method, it would have spread across all of your servers within about 10 minutes. How fast could you react?

Challenge #4: Knowing How Much Protection Is Enough

Cybersecurity professionals have an awfully difficult job. They can't just be good. They have to be impeccable. Your colleagues doing application development, service desk operations, or infrastructure management can afford to be slightly less than perfect. But people in cybersecurity? The must be nearly perfect nearly all the time. Good is not good enough.

In your company, you probably cover all of the most common pieces of the cybersecurity jigsaw puzzle. But is there still a chance you have a piece missing in your puzzle? You might locate that vulnerability through penetration testing, but will you fix the issue before the bad guy finds it?

This has recently happened to several high-profile companies. In March 2017, the Open Software Foundation publicly announced there was a major vulnerability in a version of Apache Struts. Cyber professionals in companies just like yours were not asleep at the wheel. They knew what they had to patch the vulnerability. But it was a production environment, so they had to plan carefully and execute the requisite regression testing, first running it in a sandbox to make sure there were no unintended consequences.

It took the pros a couple of months to patch that vulnerability, a common duration in the industry. The cyber experts knew it. And so did the bad guys. Both sides knew it would take a sizeable amount of time to patch a major production solution. And as they were racing to fix the problem, the bad guys exploitedthe vulnerability.

At this point, some people just give up. We know many companies that have said, "We cannot possibly keep up with the attackers, so let's just accept the inevitable." The say, "We know we're going to be breached, so we're just going to buy insurance and make sure that our company doesn't suffer financially."

You might choose that strategy. But that "solution" drives the wrong behavior within your company. Without an adequate focus on security, your employees may continue to click on live links they shouldn't be clicking on. They won't do their best to attend security awareness classes or avoid downloading vulnerabilities or viruses. Complacency fosters this unhelpful mindset.

Yes, we strongly recommend cyber insurance. But we emphatically believe that no company can rely on that alone to protect their bottom line. Without adequate measures to contain a cybersecurity compromise, the company has lost before it even steps on the battlefield.

Challenge #5: Knowing Where the Threat Is Coming From

In the Dark Ages, royals simply tried to keep the bad guys out. When they built their castles, they fortified these strongholds with high walls that enemies couldn't breach with ladders. The enemy then developed catapults that could sling boulders over the walls to mount a siege. The kings responded with stronger, higher walls. Then the enemies innovated further. Eventually, the walls couldn't be built any taller.

We have seen the same dynamic play out in cybersecurity. First, IT teams attempted to detect malware and block it. But then we discovered that a lot of the attacks were coming from inside our walls rather than from the outside.

The classic example is the Edward Snowden compromise. Snowden had privileges, including an ID and a password, and he was allowed to download sensitive data as part of his job. But he didn't have the highest level of NSA privilege (Special Access Privilege), so he installed a keystroke logger on his machine and asked one of his colleagues with a higher privilege level for help with a problem. "Could you come over to my machine — and log in with your credentials — to see if it's a problem with my workstation?" Snowden's colleague tried to help. He logged in to Edward's machine without realizing his keystrokes were being recorded. And, of course, the rest is history.

Overcoming Challenges: Elevate Your Cybersecurity Strategy

Given the ongoing pace of change and the overwhelming number of attacks, all SMEs should be continually seeking new and better ways to combat these threats. Many are doing just that and embracing software-as-a-service (SaaS) or other cloud-based solutions to improve their cybersecurity strategy.

To be effective, such options must utilize the very best end-point solutions and remain current evolve to confront the ever-evolving threat. The leading software suites in this area — including the solution offered by Integrated Cyber Solutions — do exactly that, offering a comprehensive and integrated service that not only complements but elevates enterprise defense.

Schedule A Demo

If the cybersecurity challenges presented in this whitepaper are plaguing your organization, now is the time to consider partnering with Integrated Cyber Solutions. Their solution has been proven in the real world and, best of all, can be test driven during a free 30-day trial.

The initial implementation is simple: they send you a plug-and-play device that auto-discovers your network, begins scanning for vulnerabilities, and prepares an executive report that you can view via the portal. From there, protection protocols are established, their team works to improve threat response, and your network will be better safeguarded than ever before. 98% of companies who try this solution end up adopting it within their enterprise.

If this sounds like something that could help you overcome your greatest cybersecurity challenges, please call (212.634.9534) or email (info@integrated-cyber.com). You can also learn more here.

Membership Services

Founded in 2013, the Institute for Robotic Process Automation and Artificial Intelligence (IRPA AI) is an independent professional association and knowledge forum for the buyers, sellers, influencers, and analysts of robotic process automation, cognitive computing, and AI. Our global network and advisory services offer leading-edge market intelligence, industry research, sourcing assistance, and events, as well as offering opportunities to learn and network with stakeholders across service industry functions. Email us to learn about our below services:

- Close & low cost, trained and experienced RPA & AI development talent on-demand
- AI for end-user application and device support and IT infrastructure management
- Sponsoring IRPA AI Chapters
- Sponsorship, sales and marketing programs
- Process discovery/process led automation
- Automation/AI Strategy Development
- Consulting & Program Assessment
- Vendor/Technology Selection Assistance
- Implementation Governance and ROI Achievement
- Reduce costs by streamlining unstructured and semi-structured data via automation
- Training, recruiting & certification