10 Common IT Security Risks in the Workplace

As I meet with different customers daily. I like to ask them about their key challenges. The one with the most frequency that I hear over and over is keeping their business going uninterrupted by cyber attacks and other security incidents.

Pick up any newspaper or watch any news channel and you hear about "breach du jour". What I hear come through when a new breach is announced is how most companies

continue to stay vulnerable irrespective of their sector, size, and resources.

From my perspective, there are two forces at work here, which are pulling in different directions:

- the attackers, who are getting better and faster at making their threats stick
- And the companies, which still struggle with the overload in urgent security tasks.

We've all seen this happen, but the PwC Global Economic Crime Survey 2016 confirms it:

- Cybercrime climbs to 2nd most reported economic crime affecting 32% of organizations.
- Internet-delivered attacks are no longer a thing of the future. They're an impactful reality, albeit an untouchable and often abstract one.

Top security threats can impact your company's growth

Vulnerabilities in your company's infrastructure can compromise both your current financial situation and endanger its future. Companies everywhere are looking into potential solutions to their cybersecurity issues, as The Global State of Information Security® Survey 2017 reveals.

Integration seems to be the objective that CSOs and CIOs are striving towards. Getting all the ducks in a row could paint a clearer picture in terms of security risks and vulnerabilities – and that is, indeed, a must-have. So amid this turbulent context, companies desperately need to incorporate cybersecurity measures as a key asset. It's not just about the tech, it's about business continuity.

If you are concerned with your company's safety, **there are solutions to keeping your assets secure**. The first step is to acknowledge the existing **cybersecurity risks** that expose your organization to malicious hackers.

Corporate cybersecurity risks to prepare for

Information security is a topic that you'll want to place at the top of your business plan for years to come. Having a strong plan to protect your organization from cyber attacks is fundamental. So is a business continuity plan to help you deal with the aftermath of a potential security breach.

Below you'll find a collection of IT security risks in no particular order that will be helpful as you create an action plan to strengthen your company's defenses against aggressive cyber criminals and their practices.

1. **Failure to cover cybersecurity basics**

The common vulnerabilities and exploits used by attackers in the past year reveal that fundamental cybersecurity measures are lacking. Cyber criminals use less than a dozen vulnerabilities to hack into organizations and their systems, because they don't need more.

- **The top 10 external vulnerabilities accounted for nearly 52% of all identified external vulnerabilities** Thousands of vulnerabilities account for the other 48%.
- **The top 10 internal vulnerabilities accounted for over 78% of all internal vulnerabilities during 2015.** All 10 internal vulnerabilities are directly related to **outdated patch levels** on the target systems.

Source: 2016 NTT Group Global Threat Intelligence Report

For example, something as simple as timely patching could have blocked 78% of internal vulnerabilities in the surveyed organizations. And the same goes for external security holes. Moreover, relying on antivirus as a single security layer and failing to encrypt data is an open invitation for attackers. It just screams: "open for hacking!"

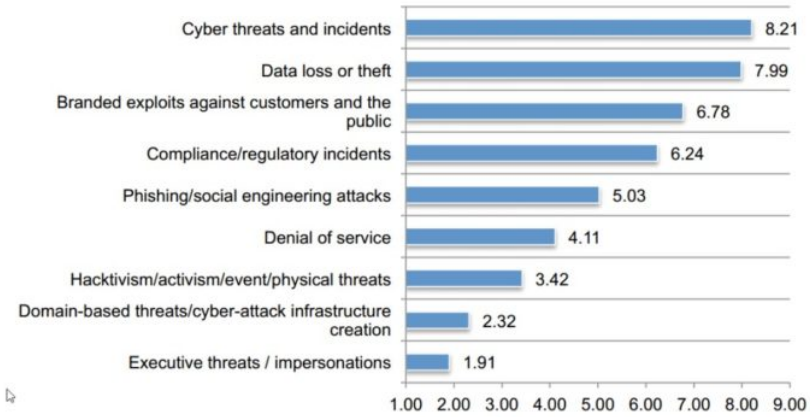
2. **Not understanding what generates corporate cybersecurity risks**

Companies often fail to understand "their vulnerability to attack, the value of their critical assets, and the profile or sophistication of potential attackers". This issue came up at

the 2015 World Economic Forum and it will probably still be relevant for a few more years.

Security risks are not always obvious. The categories below can provide some guidance for a deliberate effort to map and plan to mitigate them in the long term.

Figure 3. The likelihood of nine external threat vectors occurring
9 = most likely to 1 = least likely



Source: Ponemon Institute – Security Beyond the Traditional Perimeter

Technology isn't the only source for security risks. Psychological and sociological aspects **are also involved.** This is why company culture plays a major role in how it handles and perceives cybersecurity and its role.

3. **Lack of a cybersecurity policy**

Security standards are a must for any company that does business nowadays and wants to thrive at it. Cyber criminals aren't only targeting companies in the finance or tech sectors. They're threatening every single company out there.

The increasing frequency of high-profile security breaches has made C-level management more aware of the matter. This is an important step, but one of many. External attacks are frequent and the financial costs of external attacks are significant. The 505 enterprises and financial institutions surveyed experienced an average of **more than one cyber attack each month and spent an average of almost $3.5 million annually to deal with attacks.**

Source: Ponemon Institute – Security Beyond the Traditional Perimeter

Not prioritizing the **cybersecurity policy** as an issue and not getting employees to engage with it is not something that companies nowadays can afford. This piece of advice shared in an article on *Fortune.com* is worth considering: Just as companies seek outside expertise for legal and financial matters, they should now be looking for experts in cybersecurity and data privacy.

As part of their cybersecurity policy, companies should:

- identify risks related to cybersecurity
- establish cybersecurity governance
- develop policies, procedures, and oversight processes
- protect company networks and information
- identify and address risks associated with remote access to client information and funds transfer requests
- define and handle risks associated with vendors and other third parties
- be able to detect unauthorized activity.

4. **Confusing compliance with cybersecurity**

Another risk businesses have to deal with is the confusion between compliance and a **cybersecurity policy**. Ensuring compliance with company rules is not the equivalent of protecting the company against cyber attacks. Unless the rules integrate a clear focus on security, of course.

Enterprise risk management requires that every manager in the company has access to the parts of the security system that are relevant to them. Security is a company-wide responsibility, as our CEO always says. As a result, managers (and everyone else) should oversee how data flows through the system and know how to **protect confidential information** from leaking to cyber criminal infrastructure.

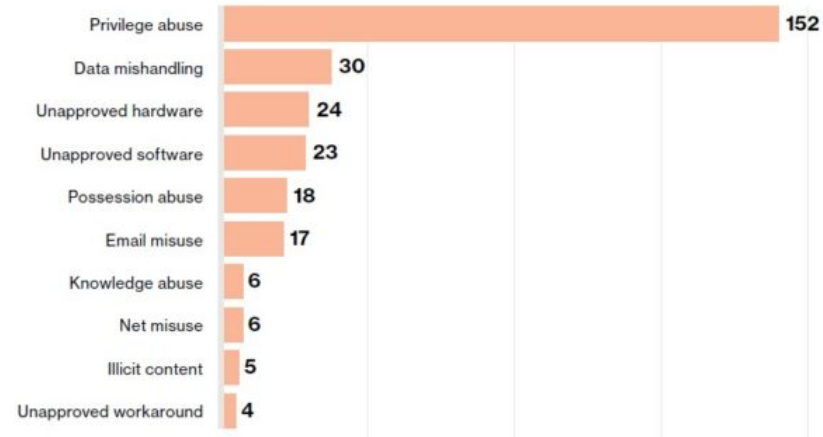
Most companies are still not adequately prepared for – or even understand the risks faced: **Only 37% of organizations have a cyber incident response plan.** Clearly, there is plenty of work to be done here.

Source: PwC Global Economic Crime Survey 2016

5. **The Carbon Lifeform – the weakest link**

There are also other factors that can become corporate cybersecurity risks. They're the less technological kind. The human factor plays an important role in how strong (or weak) your company's information security defenses are. It turns out that people in higher positions, such as executive and management roles, are less prone to becoming malicious insiders. It's the lower-level employees who can weaken your security considerably. Be mindful of how you set and monitor their access levels.

As you can see for this recent statistic, **privilege abuse** is the leading cause for data leakage determined by malicious insiders.



Source: Verizon 2016 Data Breach Investigations Report

That is one more reason to add a **cybersecurity policy** to your company's approach, beyond a compliance checklist that you may already have in place. Protecting sensitive information is essential, and you need to look inside, as well as outside to map and mitigate potential threats.

6. **Bring your own device policy (BYOD) and the cloud**

In the quest to providing your employees with better working conditions and a more flexible environment, you may have adopted the **"Bring Your Own Device" policy**. *But have you considered the corporate cybersecurity risks you brought on by doing so?*

The BYOD and Mobile Security 2016 study provides key metrics:

- **One in five organizations suffered a mobile security breach**, primarily driven by malware and malicious WiFi.
- **Security threats to BYOD impose heavy burdens on organizations' IT resources** (35%) and help desk workloads (27%).
- Despite increasing mobile security threats, data breaches and new regulations, **only 30% of organizations are increasing security budgets for BYOD in the next 12 months**. Meanwhile, 37% have no plans to change their security budgets.

The bright side is that awareness on the matter of BYOD policies is increasing. When it comes to mobile devices, **password protection** is still the go-to solution. Overall, things seem to be going in the right direction with BYOD security. But, as with everything else, there is much more companies can do about it.

7. **Funding, talent and resources constraints**

We know that there are plenty of issues to consider when it comes to growing your business, keeping your advantages and planning for growth. So budgets are tight and resources scarce. That's precisely one of the factors that incur corporate cybersecurity risks. Think of this security layer as your company's immune system. It needs funding and talent to prevent severe losses as a consequence of cyber attacks.

A good approach would be to set reasonable expectations towards this objective and allocate the resources you can afford. It won't be easy, given the shortage of cybersecurity specialists, a phenomenon that's affecting the entire industry.

Source: Cybersecurity Jobs, 2015 – Burning Glass Technologies Research

8. **No information security training**

Employee training and awareness are critical to your company's safety. In fact, **50% of companies believe security training for both new and current employees is a priority**, according to Dell's Protecting the organization against the unknown – A new generation of threats.

The specialists' recommendation is to take a quick look at the most common file types that cyber attackers use to penetrate your system. This will tell you what types of actionable advice you could include in your employees' trainings on cybersecurity. The human filter can be a strength as well as a serious weakness. **Educate your employees**, and they might thank you for it. This training can be valuable for their private lives as well.

Source: The Global State of Information Security® Survey 2017

9. **Lack of a recovery plan**

Being prepared for a security attack means to have a thorough plan. This plan should include what can happen to prevent the cyber attack, but also how to minimize the damage if is takes place. Unfortunately, the statistics reveal that companies are not ready to deal with such critical situations:

Observing the trend of incidents supported since 2013, there has been **little improvement in preparedness In 2015 there was a slight increase in organizations that were unprepared** and had no formal plan to respond to incidents. Over the last three years, an average of 77% of organizations fall into this category, leaving only 23% having some capability to effectively respond.

Source: 2016 NTT Group Global Threat Intelligence Report

If 77% of organizations lack a recovery plan, then maybe their resources would be better spent on preventive measures. This way, companies can detect the attack in its early stages, and the threats can be isolated and managed more effectively. But that doesn't eliminate the need for a recovery plan. There's no doubt that such a plan is critical for your response time and for resuming business activities.

10. **Constantly evolving risks**

There is one risk that you can't do much about: the polymorphism and stealthiness specific to current malware.

Polymorphic malware is harmful, destructive or intrusive computer software such as a virus, worm, Trojan, or spyware. Its key asset is that it can change constantly, making it difficult for anti-malware programs to detect it. That is why you should take into account that your company might need an extra layer of protection, on top of the antivirus solution.

Your first line of defense should be a product that can act proactively to identify malware. It should be able to block access to malicious servers and stop data leakage. Part of this preventive layer's role is to also keep your system protected by patching vulnerabilities fast. As cyber risks increase and cyber attacks become more aggressive, more extreme measures may become the norm. Such tactics include shutting down network segments or disconnecting specific computers from the Internet.

As this article by Deloitte points out: This may require a vastly different mindset than today's perimeter defense approach to security and privacy, where the answer is sometimes to build even higher castle walls and deeper moats.

One more thing to consider here is that cyber criminals have strong, fully automated systems that they use. Automation is crucial in your organization as well, given the sheer volume of threats that CIOs and CSOs have to deal with. You'll need a solution that scans incoming and outgoing Internet traffic to identify threats. It should also keep them from infiltrating the system. Criminals are all automated and the only way for companies to counter that is to be automated as well to find those vulnerabilities…the bad guys only have to find one hole. **We have to find them all**.

Author Bio: Larry Bianculli is managing director of enterprise and commercial sales at CCSI. He has 20 plus years experience in the IT Industry helping clients optimize their IT environment while aligning with business objectives. He is a cyber security consultant and holds a CCIE and CISSP. He has a vast experience in many verticals including Financial, Public Sector, Health Care, Service Provider and Commercial accounts. He has helped customers and lead teams with a balanced approach to strategy & planning, execution, and personal principles.

Share this post

PREVIOUS

Wireless Penetration Testing: What You Should Understand

NEXT

Cybersecurity Trends That Shook 2017

Related Posts

Cyber Safety Educatio Four Tips For Building Online Resilienc

August 4, 2021

5 Trends in Compute Science Researcl

July 28, 2021

7 Cyberse Tips for Remote Working

July 26, 20

Online Privacy and Security: The Benefits Using Resident Proxies

July 16, 2C

How to Improve Cyberse for Your Business

July 7, 202

How to Protect Healthca Data fro Ransom Attacks?

June 24, 2

Solutions

Infrastructure

Cloud

Cybersecurity

Observability – Visibility as a Service (VaaS)

Security Operations Center (SOC)

Penetration Testing

Proof of Concept Lab

Industries

Education

Enterprise

Financial

Healthcare

Media

Public Sector

Support

Why CCSI?

Careers

Contact Us

Events

Resources

Purchasing Contracts

Testimonials