CYBER SECURITY

COMPCITI
Business Solutions Inc.

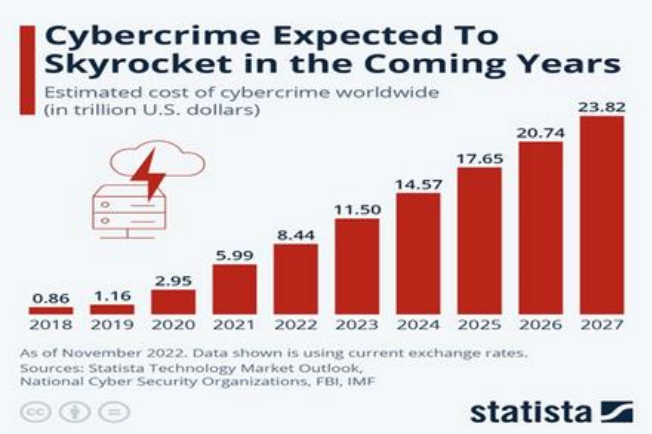
CYBERSECURITY OUTLOOK

Protection Guide for Everyone

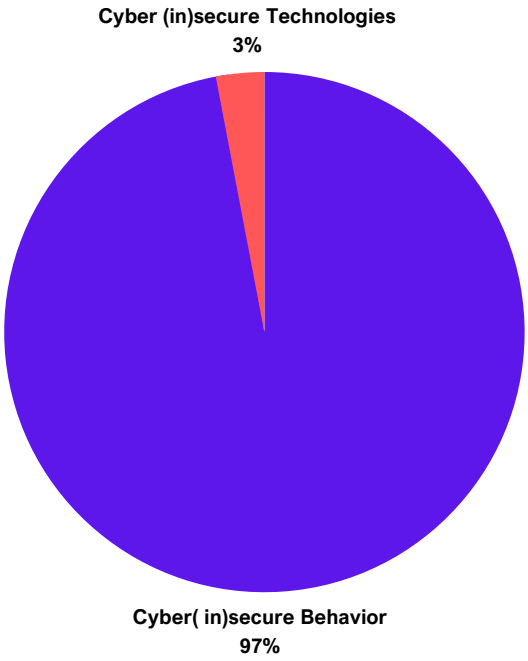
Ultimately, cybersecurity is not about technology. It's about people and (...) culture

Source" Jen Easterly, Director, Cybersecurity Infrastructure Security Agency (CISA)

Click here to watch the video



According to estimates from **Statista's Cybersecurity Outlook**, the global cost of cybercrime is expected to surge in the next five years, rising from $8.44 trillion in 2022 to $23.84 trillion by 2027.



Cause of Cyber Breaches: source: "Terrifying Cybercrime Statistics- Protect Yourself in 2021- SafeAtLast.co Cyber (in) secure Behavior, 97%, Cyber (in)secure Technologies, 3%.

In 2019, 25% of small to medium-sized businesses (SMBs) filed for bankruptcy after a cybersecurity breach.

Moreover, statistics on hacking note that 10% completely stopped doing business.

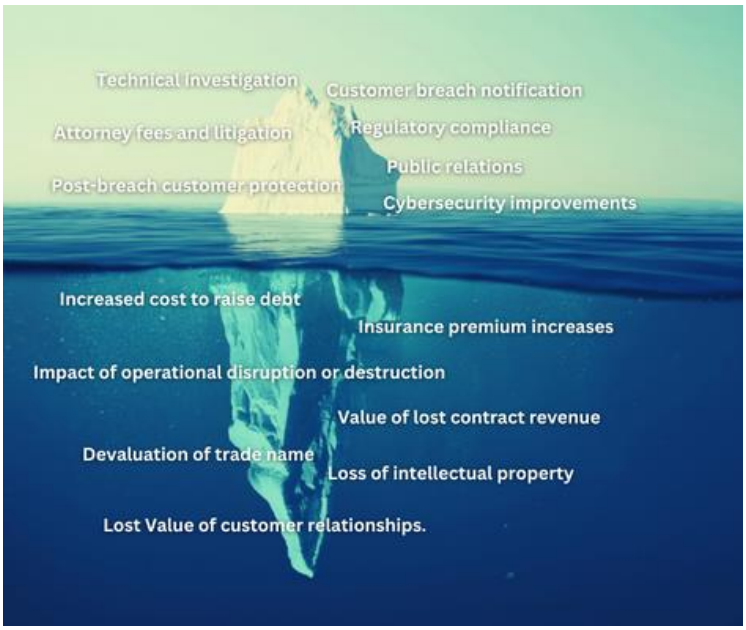
So, businesses can take many steps to reduce their risk of a security breach, including implementing strong security measures, training employees in security best practices, and regularly monitoring their systems for signs of activity.

Cybersecurity breaches predominantly result from behavior-related issues rather than technology or weaknesses within the roles of CISO (Chief Information Security Officer) or CTO (Chief Technology Officer). These behavior-related issues account for approximately 70% to as high as 97% of all breaches, whereas only a minimal 3% of breaches stem from insecure technology or technical weaknesses falling under the responsibility of the CTO/CISO/CIO (Chief Information Officer).

Around 70% to as much as 97% of all breaches occur due to behaviors related to cybersecurity that lack proper security measures, rather than being a result of technological

Shortcomings in the CISO's Role

Only 3% of breaches are linked to technical vulnerabilities within the CISO's scope. To address this, our company offers a comprehensive solution promoting behavioral change among employees, preventing 97% of breaches through heightened awareness.



This photo clearly demonstrates... "What does a cyberattack really cost? Regulatory fines, public relations costs, breach notification and protection costs, and other consequences of large-scale data breaches are well- understood. But the effects of a cyberattack can ripple for years, resulting in a wide range of "hidden" costs-many of which are intangible impacts tied to reputation damage, operational disruption or loss of proprietary information or other strategic assets."
source: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

How much is cybercrime costing your organization annually?

- $8 trillion USD a year
- $667 billion USD a month
- $154 billion USD a week
- $21.9 billion USD a day
- $913 million USD an hour
- $15.2 million USD a minute
- $255,000 USD a second

source: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Small Business

“There are 30 million small businesses in the U.S. that need to stay safe from phishing attacks, malware spying, ransomware, identity theft, major breaches and hackers who would compromise their security” says Scott Schober, author of the popular books “Hacked Again” and “Cybersecurity Is Everybody’s Business.”

More than half of all cyberattacks are committed against small-to-mid-sized businesses (SMBs), and 60 percent of them go out of business within six months of falling victim to a data breach or hack.

Small and medium sized businesses lack the financial resources and skill set to combat the emerging cyber threat.

A Better Business Bureau survey found that for small businesses — which make up more than 97 percent of total businesses in North America — the primary challenges
for more than 55 percent of them in order to develop a cybersecurity plan are a lack of resources or knowledge.

Ransomware attacks are of particular concern. “The cost of ransomware has skyrocketed and that’s a huge concern for small businesses — and it doesn’t look like there’s any end in sight” adds Schober.

COMPCITI
Business Solutions Inc.

Cybercrime Facts and Statistics

1. You have a 27.9% chance of experiencing a data breach of at least 10,000 records.

With 6,466,440 records breached every day worldwide, this should come as no surprise. The threat is real and affects individuals and businesses alike. In both cases, the best steps to take are the following: act quickly, seek help, and stop the problem from spreading. The quicker the recovery, the less it will cost you, especially if you're a small business. Unless you play it smart, you might not recover.

2. It takes organizations around 197 days to detect a breach.

Cybersecurity statistics from 2018 by the Ponemon Institute provided this invaluable insight. The mean time to contain the breach (MTTC) was 69 days. Companies that contained a breach in less than 30 days saved over $1 million.

3. The average total cost of a data breach is $3.86 million, and the average total one-year cost increase is 6.4%.

According to the Ponemon Institute, the overall cost of a data breach involves many more losses than you can imagine. There are the business disruption and revenue loss from system downtime, the lost customers that no longer trust your brand, the new customers you will fail to acquire, and finally, the lawsuits.

4. 58% of the victims are categorized as small businesses.

Organizations with fewer than 250 employees are considered small businesses. Most people are surprised to hear that small businesses are hackers' primary targets, but according to data on recent cyber security breaches, it's true. These incidents never hit the news, which is probably why they're so invisible. Remember the Target breach when tens of millions of people lost their credit card details to hackers?

Here's what most people don't know: Target's network was infiltrated via a small HVAC company. The attackers then stole access credentials to Target's network. Small businesses lack sufficient security measures and, most of all, properly trained personnel. They also neglect to back up their files or data (ransomware bait right there). And finally, they are often leveraged so that bigger companies can be hacked.

5.Devastating Impact of Cyber Attacks on Small to Mid-Sized Businesses

60% of small to mid-sized businesses forced to suspend operations after a cyber attack never recover enough to reopen. Within 6 months of such an attack, most businesses of this size struggle to bounce back due to limited resources. Lack of proper insurance coverage and means to pay ransom leave them vulnerable. Moreover, handling damage to their reputation becomes challenging. The IT department has to manage user identities, device security, networks, and cloud services across 4 separate platforms, further complicating their recovery efforts. Cybersecurity breaches can be detrimental, costing these businesses everything.

6. A malicious email was the source of the installation of 49% of non-POS malware.

Social engineering seems to be hugely successful at extracting data. One of the most significant takeaways from this report is that phishing and pretexting represent 93% of social attack-based breaches. Email breaches continue to be the most common vector for launching social attacks, with 99% of the actors being external to organizations. 59% of phishing and pretexting attacks are motivated by financial gain, with an additional 38% attributed to corporate espionage.

7. It takes 228 days, on average, for a company to even realize it's been hacked.

That's one of the most frightening **cybersecurity statistics**, since criminals can mess around with your confidential data for months on end before you even notice something's wrong, and start fixing the damage.

8. People in 86% of organizations click on phishing emails.

When talking about the general population that cannot be trained by companies, including customers, the stats are worrying. People tend to believe these pretend links are legit, and a fake website you might be led to is dangerous to an untrained eye.

9. 75% of malware in 2021 was delivered by email.

One of the most important cyber crime statistics and trends today is that hacking is becoming less and less prevalent as a technical problem. And as Medium noticed, using humans as the weak link is a growing trend, and it's becoming more and more expensive and difficult to raise awareness of employees worldwide.

10. 66% of small businesses suffered a cyberattack

This affects them a great deal, since many of them go out of business within the first couple of months of being hacked. These business cybercrime statistics matter a great deal when you have a small client base, and your reputation matters a great deal.

How to protect your company against hackers

Although executing cyberattacks on different firms is continuously improving, the firms can significantly avoid the damages by implementing cybersecurity best practices.

Implementing them isn't so difficult either. All you need to is to take care of basic security measures like:

- Setting up strong passwords to all company accounts. Say no to the "admin123" trend.
- Backup your data regularly on clouds.
- Limit access to backups to the relevant and educated IT personnel only.
- Ensure each and every system on your company network goes through regular virus scans.
- Ensure that each and every software running on your company network is up-to-date.
- Protect your company's network (including public WiFi) from unsolicited connections.
- Perform a thorough background check of every employee or potential candidate before hiring to prevent insider threats.
- We need to address the weakest link in the chain, i.e. culture. A cultural shift is required to combat the cyberthreat that is looming large on your organization.

COMPCITI
Business Solutions Inc.

90%

of data breaches start with an employee mistake

What are you doing about it?

Is it not time to provide education and empowerment to your employees, enabling them to safeguard your business?

Train your staff for cybersecurity best practices. Primarily, make them aware of phishing emails.

CompCiti can be your ultimate partner for learning and awareness training, enabling a transformation in employee behavior and fostering a robust human firewall.

cyberaware@compciti.com

CompCiti.com/cyberaware-security

COMPCITI
Business Solutions Inc.