Cybersecurity and the Internet of Things.

Tackling security threats in a data-driven world.

CSI LEASING

Introduction

Humankind gradually stepped into the industrial revolution. From one era to the next, we have adopted new ways of navigating and thriving in day-to-day life. **However, the days of gradual steps are over as we quickly leap into the fifth industrial revolution.** We've seen more change in the past two decades than ever before, specifically with the development of the internet, Big Data (BD), Artificial Intelligence (AI) and the Internet of Things (IoT).

With the emergence and dominance of Big Tech, businesses across most industries have been forced to shift their strategies and adopt new ways of working. Worldwide adaptation and evolution are widespread as new technologies are adopted and integrated into daily operations. However, the pace of change within the sphere of tech, and the challenges that surface, as a result, has caught businesses off guard. **Never before has flexibility been so important to thrive in today's fast-moving marketplace.**

CSI Leasing has worked with IDC Research to analyze the increasing threat of cybersecurity attacks on businesses all over the world. The risk of cyberattacks has been fueled by the global pandemic and the subsequent shift toward hybrid "work from home" models.[1] Cyberattacks may also be promulgated by global terrorists or even state-sponsored actors.

What has become abundantly clear is that most businesses do not have an effective, highly functional IT infrastructure network.

It is reported that a company receives **150,000 malware attacks each day,** and on average, **500 cyberattacks per year.**

The average cost of a successful cyberattack varies between $2 million and $6 million and takes around **100 days to resolve.**[1]

Let's explore the various forms of cybersecurity threats and the importance of flexibility when it comes to adopting new, robust and agile IT infrastructure.

[1] IDC Data Security Infographic - Cybersecurity in a New Accelerated World, 2021

Managing Threats in the Modern World

In 2022, businesses will be faced with a new wave of challenges. The collection and storage of data have become so essential to the way a company operates that a targeted attack on such information can result in catastrophic consequences to supply chains, employees and ultimately, profitability.

It is vital that every business understands the variety and sheer volume of cyber threats underway at this very moment. A recent report by the European Union Agency for Cybersecurity (ENISA) highlighted the 'most popular' forms of cyber threats across EU nations.[2]

Ransomware

Cybercriminals launch a malicious attack on an organization's data and demand payment to restore access. From April 2020 to July 2021, the average ransom demand doubled.

Email Attacks

A consequence of COVID-19 was a huge spike in password and credit card data theft.

Data breaches

Protected, sensitive or confidential data is leaked to untrusted sources. The healthcare industry and the financial public sectors have experienced a considerable increase in such activity.

Distributed denial-of-service (DDoS) attacks

Again, due to COVID-19, over 10 million DDoS attacks were undertaken to prevent users from accessing business systems to gather resources and information.

Supply chain threats

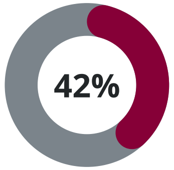
An attack targeting supply chain data and the cascading of false information. Fifty-eight percent of attackers manage to gain access to multiple data sources across the chain of businesses.

[2] ENISA threat landscape 2021

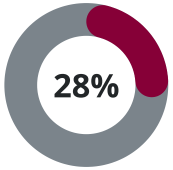
To combat cyberattacks, businesses must have a security strategy around data. Additionally, the IoT ecosystem must be updated and monitored to support the overall IT infrastructure network. By 2025, IoT connected devices are projected to reach 30.9 billion, with 15% of a company's infrastructure generated by IoT. In 2019, the total number of connected devices reached 10 million.[3] **This exponential growth in just a few years highlights the pace of change and the need to remove or upgrade outdated infrastructure.** However, modernization remains a challenge for most businesses.

One out of five companies face budget constraints when it comes to modernization.

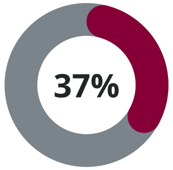
If a business delays modernization of its network, the impact could be severe:



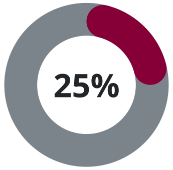
slower implementation times



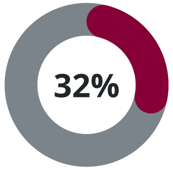
increase in lost business



more likely to experience data security breaches



more likely to receive fines for compliance issues



reduction in a company's credibility

When it comes to aging hardware, including laptops, mobile devices and on-premise servers, the risk of data breaches and cyberattacks increases.

Furthermore, it is reported that **a server will lose 14% of its performance each year,** which is why the recommendation is to update it every three to four years. However, **only 26% of businesses would *consider* a server refresh.[1]**

In addition, having 'state-of-the-art' equipment ensures that businesses are in line with GDPR regulations. As mentioned in the IDC's 'A Practical Guide to GDPR' report: "Data Protection Impact Assessments (DPIAs) require organizations to evaluate the impact of technology that could have a high risk to the rights of data subjects. These articles are aimed at embedding consideration of data protection at every stage of technology life cycle, from design and introduction, through ongoing change management, to end of life."[4]

There may be an element of complacency across businesses, which is understandable, although it is not justified given the varying threat levels. However, what is also crucial to consider is the number of skilled employees who have the knowledge, experience and authority to mitigate these risks. The array of challenges brought about by cyberattacks are a consequence of technological growth; businesses also need to be sure that its workforce is sufficiently trained and equipped to implement preventative, flexible and durable tactics.

[1] IDC Data Security Infographic - Cybersecurity in a New Accelerated World, 2021

[2] ENISA threat landscape 2021

[3] IoT Analytics Survey, November 2020

[4] IDC Report: A Practical guide to GDPR

The Hybrid-Model Goes Mainstream

The evolution of hybrid work-from-home models is a double-edged sword for businesses. Of course, it grants employees more flexibility and freedom and *should* create a happier, healthier workforce. However, to accommodate a shift in operations as a result of the Covid-19 pandemic, **the digital landscape of most businesses had to change swiftly, which ultimately left companies vulnerable to cyberattacks.**

Due to the stretched resources of IT and cybersecurity teams and a reduction in communication due to remote working, conflicts have arisen. According to the UK Government's 'Cyber Security Breaches Survey 2021,' businesses experienced inconsistencies and competing priorities. **Internal teams were balancing "IT service continuity and maintenance work, and aspects of cybersecurity such as patching software."**[6]

Due to this inconsistent focus and increased number of employees working from home, companies have reported an 80% increase in cyberattacks.

As a result, 38% of organizations have committed to further injections of spending into IT hardware, recruitment, and active measures to mitigate cyber threats [1].

[1] IDC Data Security Infographic - Cybersecurity in a New Accelerated World, 2021

[6] UK Government: Cyber Security Breaches Survey 2021

One core concern of businesses is how employees use devices and how seriously they take cybersecurity. It's thought that **65% of workers lend devices to other colleagues, and 37% do not use automatic locking settings on equipment.**

To combat a company's complacent culture, more and more IT Decision Makers (ITDM) are shifting their priorities to ensure data security is at the top of their list.

A Global Security Skills Shortage

For years, there have been ongoing discussions around skill shortages across a vast and varied range of industries. However, when it comes to recruiting experienced, skilled individuals in the cybersecurity and IT sector, time is up. The skills shortage makes it unfathomably difficult for businesses to implement specific tasks that will help manage the increase in cyber threats. **Put simply; there aren't enough people with the right training and experience to update assets and upgrade IT infrastructure.**

According to global recruitment firm Harvey Nash's 'Digital Leadership Report 2021,' cybersecurity is the most sought-after tech skill. This is followed by big data analysts, technical architects and developers.[4]

Most businesses are trying to fill this gap by cross-training current staff and hiring contractors to cover specific activities. Although this may be beneficial as a reactive strategy in the short term, it's not the best long-term strategy; particularly when tackling the larger, more time-consuming tasks such as system upgrades. In addition, by stretching current IT teams too thinly, mistakes are more likely to be made.

A further point highlighted by ENISA was that 50% of non-malicious cyber threats were due to misconfiguration of systems and, in some cases, involved broader damage to IT infrastructure. **Effectively, these cyberattacks were successful because of human error inside an organisation.**

44%

of European companies use obsolete technology [1]

65%

of security breaches exploit vulnerabilities in outdated infrastructure [1]

54%

reduction in the cost of a cyberattack, by updating infrastructure [1]

[1] IDC Data Security Infographic - Cybersecurity in a New Accelerated World, 2021

[4] Harvey Nash: Digital Leadership Report 2021

As reported in CIO magazine, IT teams experienced a 5% overall reduction in spending as the pandemic hit in 2020. In 2022, spending has not yet returned to pre-COVID norms; however, as aptly observed by CIO, "we are surfacing from crisis mode" and looking at the landscape more clearly.[5]

If businesses are to implement infrastructure upgrades, they must review recruitment strategies to look for specific skills, for instance:

Sensitive Data:

The adoption of AI and machine learning (ML) has brought about the requirement for experienced individuals to manage sensitive data workloads.

On-premises Infrastructure:

Although cloud-based systems are growing in popularity, most businesses operate under a hybrid model, with physical servers on work premises. Ideally, individuals must be experienced in monitoring and managing servers to ensure the entire IT infrastructure network is backed up effectively.

Cloud Solutions:

Individuals must be experienced in rolling out secure, encrypted, and efficient cloud-based software.

[5] CIO Magazine: Sharp IT budget cuts expected in wake of COVID-19

IT Asset Disposal (ITAD)

Many companies don't necessarily have a robust strategy when it comes to IT disposal. Older assets are often discarded with the procurement of newer models. But the ongoing need to update equipment in order to remain competitive should not absolve companies from disposing of older equipment in a safe and environmentally friendly way.

Old data-bearing hardware should be data wiped to globally recognised standards such as NIST 800-88 to ensure the protection and erasure of personal data in line with GDPR legislation. With more and more people working from home and the potential for devices to fall into the wrong hands, GDPR challenges may begin to rear their heads unless companies have adequate end-of-life data destruction strategies

Sustainable disposal is a crucial element in IT lifecycle management, so it's essential to familiarize yourself with and identify the specific accreditations associated with reputable ITAD businesses.

A business with an approved external validation of assets and processes will be properly certified

CSI Leasing's ITAD business, EPC Global Solutions, h**as obtained ISO 14001, ISO 9001 and ISO 45001 certifications in Europe and ISO 14001 and e-Stewards certifications in the U.S**. They are also a **Blancco Platinum Partner** globally and have years of experience working with multiple companies to serve their IT infrastructure needs.

IT Equipment Leasing

With remote working, irregular hours, and a plethora of ‘priority tasks’, cyberattacks continue to rise as IT teams remain under the microscope.

One proven method to manage new working styles is to consider IT equipment leasing. In doing so, operational efficiency is guaranteed as the procurement of devices is outsourced, as well as asset lifecycle analysis.

As we move forward, over 36% of European companies plan to implement and accelerate a leasing model in 2022. By 2024, almost 50% of businesses will have adopted this agile, flexible strategy [1]

This approach leads to effective IT lifecycle management, enabling you to have an up-to-date infrastructure. From acquisition and management to the environmentally friendly disposal of obsolete assets, each of which is subject to certified data wiping.

There are multiple benefits of IT leasing. First, the pressure on IT teams is alleviated as they will no longer be responsible for the procurement and delivery of assets, helping to overcome the shortage of skilled staff. Second, a company can adopt a rolling replacement strategy, resulting in an end to outdated hardware, which may pose a security risk. Third, by shifting hardware from a capital expenditure to operational expenditure, the additional technology budget you need to overcome the aforementioned challenges can be spread over the useful life of the technology.

The entire network of devices can even be recorded in an asset information platform and monitored centrally, meaning guesswork is eliminated! With CSI Leasing’s MyCSI platform, businesses can manage an entire IT infrastructure network, both nationally and internationally. In addition, CSI Leasing’s Global Desk team specializes in managing large accounts and will ensure that a client has a centralized point of contact for all locations.

By having up-to-date infrastructure, the risks of cyberattacks are reduced by 23%, and a company can benefit from a 22.2% cost reduction per employee.

If you’re looking to upgrade your IT Infrastructure, or concerned about cybersecurity, CSI Leasing is available to help you and your business maintain security and productivity.

[1] IDC Data Security Infographic - Cybersecurity in a New Accelerated World, 2021