

DAMAGE CONTROL

A Guide for the Cyber
Resilient Communicator

coordinated by Mihaela Pană

National University of Political Studies and Public Administration
College of Communication and Public Relations
MA in Digital Communication and Innovation
Students' teamwork experience in Cyber Resilience coordinated by Mihaela Pană


TEAM LEADER

Clemența-Andreea Roșu (Togan)

CREATIVE TEAM

Claudio-Florin Timofei, Cătălina-Elena Albescu, Mihaela Denisa Luca,
Radu-Ștefan Bănică, Alexandra Olteanu, Alexandra-Tania Pancă,
Ana-Maria Popescu-Octav-Sargețiu, Ruxandra-Maria Chifan, Andreea-Ioana Trandafir,
Diana-Cristina Tunsu

DESIGN TEAM

Tudor Stan | Graphic Design and Layout provided by  blureo

Ilie-Răzvan Țurcanu, Andrada-Gabriela Andrei, Elena-Andreea Antonie,
Andreea-Denisia Lupoi, Dorina Mădălina Manea, Andrei-Cristian Roșu,
Maria-Alexandra Sandu

DEVELOPMENT TEAM

Teodora Avram, Ioana Georgiana Florescu, Teodora-Maria Atanasescu, Olga Dănilă,
Smaranda-Alexandra Bărbuță, Alexandra-Teodora Bardici, Mădălina-Mihaela Spiță,
Iuliana-Filofteia Perpeleac, Roxana-Gabriela Popescu

Copyright © Editura COMUNICARE.RO, 2023, for this edition.
All rights to this edition belong to COMUNICARE.RO University Press.

COMUNICARE.RO University Press is a department within the National University of
Political Studies and Public Administration, College of Communication and Public
Relations.

SNSPA, College of Communication and Public Relations
Str. Povernei, nr. 6
010643, București, România
www.edituracomunicare.ro
e-mail: editura@comunicare.ro

ISBN: 978-973-711-649-9 (ediție electronică)

comunicare  **ro**

Bucharest, 2023

CONTENTS

FOREWORD	3
I. MISSION AND VISION	4
II. INTRODUCTION TO CYBER RESILIENCE	6
2.1 Why Cyber Resilience Matters	6
2.2 Cyber Security vs Cyber Resilience	7
2.3 The Need for a Cyber Resilience Strategy	9
III. BUILDING RESILIENCE TO CYBER THREATS	12
3.1 Recognising cyber attacks	12
3.2 Protection tips depending on the type of attack	16
3.3 Vulnerabilities	17
IV. CYBER RESILIENCE FROM A CORPORATE PERSPECTIVE	19
4.1 Identifying Your Organisations' Critical Assets and Systems	19
4.2 Risk Management	20
4.3 Employee Training and Awareness Programs	22
4.4 Developing a Cyber Incident Response Plan	23
4.5 Data Backup and Recovery Plan	24
V. CYBER RESILIENCE FROM A DAILY PERSPECTIVE	27
5.1 Identifying Vulnerabilities in Your Personal Life and Ways to Respond	27
5.1.1 Personal devices	27
5.1.2 Social media	28
5.1.3 Account management	28
5.1.4 Phishing and social engineering hacks	29
5.2 Consistent Measures to Maintain Cyber Resilience in Your Personal Life	31
5.2.1 Personal Devices	31
5.2.2 Social Media	32
5.2.3 Account Management	33
5.2.4 Phishing and Social Engineering Hacks	34
5.3 Withstand: Reactions in Case of a Cybercrime	34
5.4 Recovery and Adapt: Sharing Lessons Learned with Family and Social Circle	36
VI. CONCLUSION	38
MEMORIES WALL	41
REFERENCES	44

FOREWORD

Guidance on Cyber Resilience

The challenge of teaching communication professionals to become cyber resilient is reflected in this handbook, a joint venture between first-year master's students in Digital Communication and Innovation at FCRP. Beyond the knowledge gained during the Cyber Resilience course, this guide is the Communication students' choice to tell the story further and a pathway to their own resilience toolkit for the future.

Before the first course, students had the perception that cyber resilience equals cyber security, cyberattacks and hackers. Now, they are the ones talking about anticipation, resilience, recovery and adaptation, embracing useful analogies for the communicator's critical role in managing a cybersecurity crisis, which is more important than they have imagined.

But the journey up to this point went through from becoming aware of one's own resilience responses to unknown pitfalls in an invisible environment, similar to cyber traps behind a click. Thus, the cyber resilience pillars of anticipation, withstand, recovery and adaptation were explained through an adapted analogy of the Blind Man's Bluff Game, turning the theory into an enjoyable experience. Figuring out their own natural resilience potential and identifying emotions similar to those provoked by slightly happier online experiences was the most effective way to grasp the need for resilience in cyberspace.

Monday's course became shortly the perfect time to share cyber mistakes, lessons from which we have learned together how to assess vulnerabilities, avoid threats, strengthen our cyber protection, minimize the risks, create backups, and manage emotions that are hacked online. All of this with an eye on both the personal and professional sides, being aware of the fact that in the world of interconnected systems in which we function, any misstep can have consequences where we least expect them. As professional communicators we have the damage control duty, the proof of concept behind this guide.

Cyber resilience pathfinder,
Mihaela Pană
Bucharest, 2023

Chapter 1

MISSION AND VISION

Welcome to “Damage Control” – a comprehensive guide on cyber resilience for individual users and businesses. In today’s increasingly digital world, cybersecurity is paramount, and we understand the challenges individuals and organizations face in protecting themselves against cyber threats.

The frequency and severity of cyber-attacks have risen dramatically in recent years. Cybercriminals constantly find new ways to exploit vulnerabilities and steal sensitive information, from data breaches to ransomware attacks. As technology advances and more businesses move online, the need for effective cybersecurity measures has never been greater.

But who are we?

As pioneering Master students at the forefront of the newly established program “Digital Communication and Innovation” within the Communication and Public Relations field, we are excited to create this guide on cybersecurity awareness. Our unique position as the first cohort of this innovative program equips us with a fresh perspective and a deep understanding of the evolving digital landscape.

And why us?

As Master’s students studying Communication and Digital Innovation, we possess a unique blend of knowledge and skills that make us well suited to create this guide and share valuable information on cybersecurity. Our Communication and Digital Innovation studies provide a deep understanding of the digital landscape, including emerging technologies, digital communication channels, and online platforms. This knowledge equips us to recognise the risks and vulnerabilities inherent in these environments. Furthermore, our technical expertise in various digital tools and platforms enables us to assess the cybersecurity implications of different tools and guide users on their safe and secure usage.

In addition to our technical proficiency, our education equips us to understand different cyber threats, such as malware, phishing, and social engineering. We are well-versed in the tactics employed by malicious actors and can help others identify and protect themselves against these threats.

Moreover, our studies give insights into industry best practices and trends. This knowledge allows us to provide up-to-date information and guidance on cybersecurity measures relevant to individuals and businesses.

We are committed to fostering a culture of cybersecurity awareness and responsibility. By creating this guide, we aim to share our expertise and empower you to navigate the digital landscape confidently, protecting yourself and your work from cyber threats. Knowledge allows us to provide up-to-date information and guidance on cybersecurity measures relevant to individuals and businesses.

We are committed to fostering a culture of cybersecurity awareness and responsibility. By creating this guide, we aim to share our expertise and empower you to navigate the digital landscape confidently, protecting yourself and your work from cyber threats.

Everyone has a role in cybersecurity

Whether you're an individual or part of an organization, it's essential to understand the risks and take steps to protect yourself and your assets. By offering practical advice and best practices, we hope to empower you to take control of your cybersecurity and minimize the damage caused by cyber-attacks.

We understand that navigating the complex world of cybersecurity can be challenging, so we have designed this guide to be accessible and easy to understand. Whether a beginner or an experienced professional, our guide provides valuable insights and actionable steps to improve cyber resilience. Thank you for choosing Damage Control. We hope this guide will serve as a valuable resource for individuals and organizations alike, and we look forward to helping you build a stronger, more resilient cybersecurity strategy.

We encourage you to delve into this guide, explore the topics covered, and apply the insights gained to strengthen your cybersecurity defenses. Let's create a safer digital environment for ourselves and the organizations we engage with.

Chapter 2

INTRODUCTION TO CYBER RESILIENCE



Authors' Insights Developing Resilience Means Being Aware of

Potential threats, personal defense skills, the level of danger.

Your limitations and how to overcome them.

Threats, and where the potential to avoid or face them lies.

Your power (knowledge) and how you can use it to grow or protect yourself.



2.1 Why Cyber Resilience Matters

As the world continues to become more digitized, the risk of cyber-attacks increases alarmingly. The COVID-19 pandemic has further accelerated the shift towards digitalisation, with more people working remotely and relying on digital tools to stay connected. This has created new opportunities for cybercriminals to exploit network, system, and device vulnerabilities. A successful cyber-attack can have far-reaching consequences, ranging from financial losses to reputational damage and even loss of life in critical infrastructure systems.

In this context, cyber resilience has emerged as a critical aspect of cybersecurity. In the context of complex systems, which include physical and informational domains and cognitive and social ones, cyber resilience should be considered (Smith, 2005).

Cyber Resilience, defined by the National Academies of Science (NAS), refers to the ability of a system or network to prepare, absorb, recover and adapt to adverse effects, especially those associated with cyber-attacks (Linkov & Kott, 2008). Cyber resilience is not just about preventing cyber-attacks but also about minimizing the impact of successful attacks and ensuring a quick and effective recovery.

It is no longer a question of if but rather when a cyber-attack will target an organization. In the event of a successful attack, cyber resilience can mean the difference between a minor inconvenience and a catastrophic event that puts an organization out of business. Therefore, organizations must prioritize cyber resilience as a core aspect of their cybersecurity strategy (Linkov & Kott, 2008). Ensuring cyber resilience is not just an issue for large corporations and government agencies but for any organization or individual that relies on technology to carry out its operations or daily activities. The rise of remote work and the increasing interconnectedness of devices and systems only amplifies the need for cyber resilience. To the growing sophistication of cyber threats, more is needed to focus solely on preventing attacks. Instead, organizations and individuals must also prepare for the possibility of an attack and have strategies to mitigate and recover from the effects of a cyber attack. By doing so, they can minimize the damage caused and ensure continuity of operations (Linkov & Kott, 2008).

This guide provides an overview of cyber resilience, including its definition, key components, and best practices for implementing it in an organization. By understanding the importance of cyber resilience and taking proactive steps to improve it, organizations can better protect themselves against cyber-attacks and minimize the impact of successful attacks.



2.2 Cyber Security vs Cyber Resilience

As companies and organizations become more reliant on technology, they face an increasing number of threats from cyberattacks. It's important to understand the difference between cyber security and cyber resilience. While they may seem similar, they serve different purposes in protecting your digital assets. Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from digital attacks, theft, and damage with a focus on prevention and risk reduction to minimize the impact of any cyberattack. Resilience, on the other hand, refers to the ability of individuals and organizations to withstand and recover from a potential cyber attack.

“It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it.” – Stéphane Nappo, Global Chief Information Security Officer (2020)

Among the main objectives in cyber security: protect confidentiality, integrity and availability of information; ensure compliance with rules and regulations; minimize risk by identifying weaknesses and vulnerabilities in your IT infrastructure. Security and resilience are two sides of the same coin – they both deal with risk and uncertainty. By understanding their differences and commonalities, we can create a safer, more sustainable future for ourselves and others.

“One way of thinking about the difference is that cyber resilience involves accepting the fact that no cybersecurity solution is perfect or capable of protecting against every possible form of cyber threat. This is why every company needs both aspects. The cybersecurity strategy is designed to minimize the risk of attacks getting through. But when they inevitably do, the cyber resilience strategy is there to minimize the impact.” – Bernard Marr, strategic business & technology advisor (2021)



Case Study

“Hack The Hague” is a program designed to enhance resilience and improve crisis communication in the event of a cyber attack in the Netherlands. Reflecting the growing threat from cyber criminals to organizations of all sizes, regardless of the sector in which they operate, the competition invites international professional and student hackers to attempt to hack the live IT systems, applications and websites of the municipality of The Hague.



All those taking part agree in advance to report the vulnerabilities they find in a dedicated portal, along with evidence of what they found and how they found it. Importantly, the successful hackers are encouraged to suggest ways to resolve the problems they find, without releasing any details publicly. It is an interesting and courageous response to the threats faced by organizations and suggests that no single cyber security service can address every likely issue.

Hack the Hague event organizers explain it not only helps to map and assess the municipality's attack surface, a necessary step in strengthening cyber-resilience, it also raises awareness about digital security and its importance for organizations, businesses and individuals.

There are a number of platforms, such as 'HackerOne', that allow companies to sign up, put their systems in scope in much the same way The Hague does in this annual event. If a vulnerability is identified by an ethical hacker, they can report it and potentially get paid a bounty for their work.



2.3 The Need For a Cyber Resilience Strategy

IT security experts believe that cyber threats have become so sophisticated, that preventive strategies alone are not good enough to offer protection. They believe that eventually there will be unauthorized access to their companies' systems, and they want to be prepared for this inevitability as best as they can.

"It is vital to build inside you a real human firewall to cyber threats. (...) You have a firewall that keeps bad traffic from coming into your network, you also have encryption, intrusion detection systems and monitoring systems, those are the older parts of cyber security. Secure yourself from the inside is about an evolution going on in cybersecurity." – Jonathan Reiber (INKtalks, 2019)

The successful implementation of cyber resilience depends on your cyber security culture to make safer choices on devices, technologies and digital services. IBM describes the importance of building a cyber resilience strategy as "vital for business continuity". It can provide benefits beyond increasing an enterprise's security posture and reducing the risk of exposure to its critical infrastructure. Cyber resilience also helps reduce financial loss and reputational damage. And if an organization receives cyber resilience certification, it can instill trust in its clients and customers. Further, a cyber-resilient company can optimize the value it creates for its customers, increasing its competitive advantage through effective and efficient operations.



Case Study

Cybersecurity & Infrastructure Security Agency (CISA) has created the methods and the guidance needed to secure and enhance the resilience of the nation's critical infrastructure. Their resilience services are provided through Resilience Service Branch (RSB), which has the mission to enhance security and resilience, by developing methods, capabilities and guidance for assessment of security of assets and systems, and implementation of

resilience-based approaches in local and regional planning. As RSB conducts regional infrastructure resilience assessments, CISA strengthens its partnerships with those organizations, and develops capabilities and resources which can be utilized by other stakeholders.

Conduct assessments, analysis, and support planning: lead efforts to enhance the understanding of, and drive collective action on, infrastructure security and resilience challenges – by, with, and through integrated planning and assessment capabilities to enhance resilience. The complementary processes of assessments and planning highlights RSB's unique capability to support and empower stakeholders.

CISA conducts specialized security and resilience assessments on the nation's critical infrastructure. These voluntary assessments allow them to better understand and manage risk while enabling efficient response and restoration in all post-event situations.





Authors' Insights

Being Aware of Tech Vulnerabilities Means

Continuously assessing weaknesses and patching systems to prevent the exploit of past vulnerabilities.

Assessing the vulnerabilities of your organization or system, determine what you need to address them, track them, document them and fix them.

Knowing you are exposed at any time to data breaches, software incompatibilities, accessing malware from different sources deemed as credible.

To build strong layers and protect yourself from an attack or at list, mitigate the damage.

Knowing the possible breaches of a system, a program, a product and taking measures to protect them.

Being aware enough not to let any valuable info on any device. Digitalization era does not mean it's "cooler". In fact, it is more controlling.

Knowing and understanding how, what and which are the situations that makes us vulnerable and acting accordingly.

To be able to protect yourself and build multiple layers to ensure that you are covered.

To keep your stuff safe and protect your personal data.

Chapter 3

BUILDING RESILIENCE TO CYBER THREATS



3.1 Recognising Cyber Attacks

We have to consider that in our era the subject of cybersecurity is of most importance. Since we are heavily reliant on technology in all that pertains to communication, business and prioritizing data, and its storage, in turn this increases the frequency of cyber attacks. That is the reason why recognizing and preventing threats must evolve along with technology.

This chapter of the guide will explain what are the most common types of cyber attacks, for readers to understand how they work and will further explore how to build resilience against these threats. It is important for users to understand this information and to be aware of the risks in order to build a proactive approach towards cybersecurity.

Some factors to consider are:

- ✔ There have been *“more than 20 million messages tried to deliver malware linked to an eventual ransomware attack”* (The Human Factor Report 2022 – Threat Report | Proofpoint US, 2023).
- ✔ In the report of the The Human Factor Report 2022, it has been noted that *“80% of businesses are attacked by a compromised supplier account in any given month”*.
- ✔ There are more than 100,000 attempted cyberattacks through telephones. *“SMS-based phishing attempts doubled in the U.S. year over year”* (The Human Factor Report 2022 – Threat Report | Proofpoint US, 2023).
- ✔ The median number of days an attacker is present in a target’s environment before being detected, dropped to 16 days in 2022, down from 21 days in 2021 (Mandiant Unveils M-Trends 2023 Report).

- ✔ There has been a decrease in ransomware from 23% in 2021 to 18% in 2022. Many factors could be contributing to this drop, including the conflict in Ukraine (Mandiant Unveils M-Trends 2023 Report).
- ✔ Cyber espionage and new malware families increased significantly in 2022 (Mandiant Unveils M-Trends 2023 Report).
- ✔ There is new threats incoming like “using data from underground cybercrime markets and employing social engineering techniques over voice calls and text messages” (Mandiant Unveils M-Trends 2023 Report).
- ✔ Due to cyber threat in Ukraine, government-related organizations became the main targets, “accounting for 25% of all investigations” (Mandiant Unveils M-Trends 2023 Report).
- ✔ Activity related to data theft and information has increased since 2022. (Mandiant Unveils M-Trends 2023 Report).
- ✔ The increased use of social media platforms has increased the spread of misinformation with the intention of confusing and causing uncertainty in the public, for this deep fakes and bots have been heavily used (Cybersecurity: Main and Emerging Threats | News | European Parliament, 2023).
- ✔ Since the Russia-Ukraine war there has been an increase in the “hacktivism” cyber threat Hacktivism, cybercriminals wanting to “extort money” from people who were trying to help charities in need (Cybersecurity: Main and Emerging Threats | News | European Parliament, 2023).



Case Study

Phishing attacks, the most common cyber attacks, involve sending deceptive emails or SMS to unsuspecting individuals in an attempt to trick them into revealing sensitive information or performing actions that benefit the attacker. Recently, there was a cyber attack through the Romanian Post National Company. The method used by the hackers was as follows: from a Romanian phone number, they send an SMS informing the consumer that he must receive a parcel, but the address is incorrect. Then, a link containing the words Posta Romana was indicated. After accessing the respective link, personal data was

requested (postal address, e-mail address, telephone number) and a payment interface similar to any other portal, specific to internet payments, is generated. Through it, a symbolic amount is requested. After completing the data required by the interface (card number, expiration date, cardholder, security code), the recipient receives a bank code. Hackers are actually hiding under this interface, who enter the card data into the specific application, thus stealing the money. Recognizing and comprehending prevalent types of cyber assaults is critical for developing cyber threat resistance.

iMessage
Yesterday 15:20

Poșta Română: Din cauza pierderii adresei, pachetul nu poate fi livrat. Vă rugăm să rezolvați această problemă imediat. Puteți actualiza adresa online și aplica pentru o nouă livrare: <https://posta-romana.xmrct.com/>
Vă rugăm să răspundeți la 1 pentru a activa link-ul și a actualiza adresa online și pentru a solicita o nouă livrare

The sender is not in your contact list.

Some examples of typical cyber assaults are:

1. Phishing

“Phishing is when a cybercriminal sends an email, text, or pop-up message asking for personal or financial information” (Shields, 2015, p. 349). Probably the most common type of cyber attack is Phishing. Through the use of email, texts, or certain websites, attackers can find and try to do harm by obtaining private information such as credit card numbers and passwords. Phishing was the second most utilized vector, representing 22% of intrusions. (Mandiant Unveils M-Trends 2023 Report)

2. Malware

Another major attack that can happen is malintended software being installed on a computer with the purpose to weaken the system’s protection and gain information. *“Cybercriminals can install malware, short for malicious software on computers, smart phones, or other mobile devices without the owner’s consent”* (Shields, 2015, p. 349). Some examples of names include: Viruses, worms, Trojans, ransomware, and spyware. *“60% of affected organizations may have paid ransom demands.”* (Threat Landscape, 2022)

3. Man-in-the-middle (MITM)

Can also be associated with third party vendors, and can be described as a way to attack companies or people by interception of communication between the vendor and the person or the company. This is done to steal data, it is more complicated but still effective in stealing private information. There have been cases where a company was under attack because the attackers got sensitive information by firstly cracking down the security of a third party vendor. (Shields, 2015, p. 350)

4. Zero-day attacks

These attacks are usually very hard to detect and they prey on previous vulnerabilities of certain systems. *“Zero-day attacks are considered the ultimate challenge in cyber security domain.”* (Aleroud & Karabatis, 2012, p. 40)

5. SQL injection

Another very difficult attack to find and resolve is SQL Injections. They are described as being applications that may be weakened by the attacker. In this case *“SQL injection may allow an attacker to gain complete access”* (Halfond et al., 2006, p. 1). The sensitive information gained by the attacker may result in *“identity theft, loss of confidential information, and fraud”*. (Halfond et al., 2006, p. 1)

6. Denial-of-service (DoS) and distributed denial-of-service (DDoS)

This type of attack is characterized by overloading systems with the aim of making it crash. In turn it *“attempts to block legitimate users’ system access by reducing system availability”*. (Carl et al., 2006)

7. Cross-Site Scripting (XSS)

XSS attacks inject malicious code into legitimate websites, allowing attackers to steal sensitive information or take control of the website.



Case Study

Cybercrime at the crossroads of offline and online

I still remember that night out in Centru Vechi, the old town of Bucharest. The city was alive, and I was having the best time. But in the midst of all the excitement, my night took a turn I hadn't anticipated.

I was walking in a tight corner, when from the back pocket of my jeans I felt something slip out, I turned in despair but my phone was already gone. I tried to scream out at people, panicked, but the thief ran and I couldn't do



anything. In that moment, I went to the nearest police car pleading for help, but all I heard was “Miss, sorry, these things happen all the time, you should have been more careful, tomorrow the first thing you should do is go to the station in Centru Vechi to give a statement”.

Once I got home, I hurried immediately to my laptop, changed all of my passwords, and froze my Revolut account. In disbelief I saw a payment of 100 Ron of my card at a corner store in Iancului. Someone tried to pay with the card that was sitting in the phone case. Jokes on them I had no money in the main account, since I held it in the seif of the application, I love Revolut!

The next day I went to the police station, I gave them all the info about the location of the store, but that was all I had, also the IMEI number. I hoped that the payment at the corner store could be a lead. Unfortunately, despite my best efforts, nothing came of it. The investigation hit a dead end, my phone remained lost.

This experience has taught me an invaluable lesson about personal security in the digital age. Cybercrime isn't just something you hear about in the news – it can happen to anyone. Now, I take every precaution to protect myself, my devices, and my information, and I encourage others to do the same. After all, you never think it'll happen to you, until it does. – Teodora Avram



3.2 Protection Tips Depending on the Type of Attack

1. Phishing

To protect from this attack make sure that you read and check very carefully any emails that look suspicious, look at the sender, and do not click links you do not recognize. Search the source of the email, and do not send private information. (Goutam, 2015, p. 15)

2. Malware

Malware attacks can be prevented by installing a good quality anti-virus software, updating the recommended drives and computer updates and not downloading unrecognized softwares or programs that are not licensed. Make sure to double check by simply Googling the name of the software. (Goutam, 2015, p. 15)

3. Man-in-the-middle (MITM)

It is very important for a business to do background checks on third party vendors, safeguard the data, use secure connections (HTTPS), virtual private networks (VPNs), and two-factor authentication. (Ulsch, 2014)

4. Zero-day

It is very important to keep systems updated, detect any unusual activity on the system and engage with protection programs.

5. SQL injection

A good practice to safeguard from these attacks is to update systems and patches to the latest ones.

6. DoS/DDoS

In the case of this type of attack it is important to use firewalls, detection systems to find out the source of the attack and monitoring traffic on websites or applications.

7. Cross-Site Scripting (XSS)

A way to make sure that this attack is prevented is mostly to code the output of the website to make sure that any information from users, databases, or other sources is harmless. In the case of dangerous scripts they won't be executed.



3.3 Vulnerabilities

Vulnerabilities are a doorway for attackers/hackers to find flaws in systems or apps which they will exploit to launch attacks. By identifying and fixing vulnerabilities you are creating cyber threat resistance. Some of the best practice include:

1. One of the most important and simple tactics is to update and patch software and operating systems on a regular basis. Along with this comes the “coordination of filling the security gaps in the critical computer systems” (Hruza et al., 2015, p. 3).
2. Another tactic can be to test systems and detect any possible issues or suspicious activity (vulnerability and penetration testing).

3. Along with two step factor authentication you can also transmit sensitive data by encrypting it.

4. In the case of business the training of the staff is highly recommended, workshops and courses can help in creating a strong security culture inside your firm. “Gathering the information on serious security incidents” can also be a big help in detection and prevention of attacks (Hruza et al., 2015, p. 3).

5. A plan is always needed in the case of the attack, so a strategy or a plan is most needed to make sure that the correct steps are taken and that the company can recover from attacks. “Coordination of countermeasures for IT security incidents in the critical infrastructure.” (Hruza et al., 2015, p. 3).

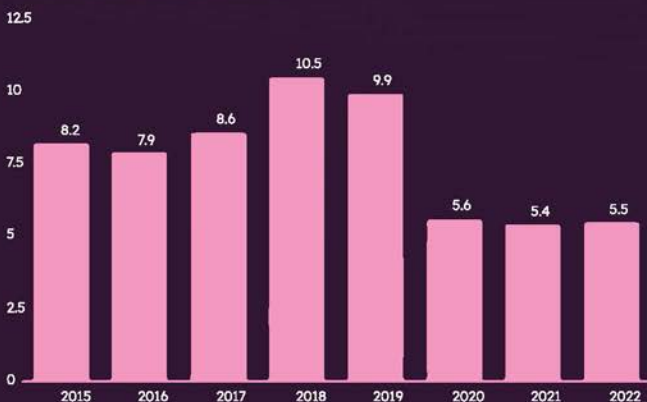
Ransomware Evolution

— Average Ransom Payment



Source: Coverware, Inc. Q1 2021 Ransomware Report

Malware Threats: graph showing the decrease in malware incidents during the peak of the Covid-19 pandemic



Source
SonicWall
©Statista 2023

Additional Information
Worldwide; SonicWall; 2015 to 2022; data is based on SonicWall Capture Labs characteristics

Chapter 4

CYBER RESILIENCE FROM A CORPORATE PERSPECTIVE

The corporate world represents an extremely significant vulnerable sector when it comes to cybersecurity and for cybercriminals it serves as an easy-to-access playground, especially in terms of economic matters, intellectual property and personal or corporate data.

In this very fast, and highly digitalized era, it is very important for corporate workers and CEO's to come together, creating a backup plan of a backup plan, a cybersecurity strategy, for an everlasting and constantly improved cybersecurity plan, that would provide a safe and thriving workflow, based on up to date protection and awareness.

As for every business, there should be a kind of supply chain, for a qualitative work flow within any business, cyber security measures should become a mandatory part of the business supply chain. (Kaplan, Weinberg, 2011, pp. 2-4)



4.1 Identifying Your Organisations' Critical Assets and Systems

Within a corporate organization, the critical assets are represented by the organization's supplies that are meant to assure an efficient activity in fulfilling the organizational purposes. (CISA, 2023)

In this case, the critical assets of a good corporate cybersecurity strategy can be tangible-technological props such as devices, software, hardware, or any tech accessory, or intangible assets such as human resources, business model, data, or intellectual property, or brand image. (Ross, Pillitteri, Graubart, Bodrau, McQuaid, 2019, p. 1)

These assets are very important factors within every cyber-threat within an corporate organization as cyber-security is becoming more and more important as the online environments and their facilities develop. These two elements, the cyber-threats and the emerging online facilities are simultaneously growing in terms of power, also as the level of online vulnerability.

So, nowadays in terms of cyber-security, a few moments have been observed:



Valuable businesses are more likely to experience more, and often attacks or they can become a real target for the cyber-attackers. The same goes for the businesses that have a large number of customers, so that means that they also have a massive database, with personal data.



Organizations are considered to be more available than they were before. The cyber-attackers are expecting that corporate workers are using the same tech devices for both work and personal use, so there is an increased level of data, and availability, especially in terms of accessing malware ready to attack corporate elements.



The supply chains within an organization are co-dependent. As an organization has its stakeholders, there is a corporate strategy for creating a strong link with these stakeholders, to join all parties into an unique network in order to improve the overall work-flow and organizational purposes. The action of creating this unique network, can threaten the cyber-security systems of all of the parties included in the network, so there is a higher level of vulnerability.



Cyber-attackers are becoming more and more experienced, damaging and subtle. When it comes to committing cybercrime; attackers have improved technologies and they have the power of impersonating political or activist entities in order to obtain financial benefits, intellectual property or business patents through “industrial espionage”, triggering and attacking organizational vulnerabilities. (Kaplan, Weinberg, 2011, pp. 2-3)



4.2 Risk Management

When it comes to cyber security and cyber resiliency within an organization, the risk management strategies are meant to fulfill organizational purposes and to reinforce the workflow. Cyber resiliency in an organization is codependent with the organizational purposes, as the cyber security and cyber resilience

strategies and their implementation should be personalized based on the business model's core needs and values.

A cyber security risk management plan should be included in the overall main corporate strategy, and the risks should be taken into consideration as much as financial risks. Within a business, there should be a plan for an eventual risk response, a strategy, where the CEOs and the corporate teams should establish their priorities and vulnerabilities in terms of cyber threat. The strategy build-up should be based on the organizational beliefs such as corporate contractual terms and conditions, organizational protocols, tactics, investments and cultural orientation. Furthermore, the risk management plan, could also be based on precedence, situations of cyber attacks, so that there can be a guideline in terms of the appropriate steps, or a hint on where to begin and what to begin with. (Ross, Pillitteri, Graubart, Bodrau, McQuaid, 2019, pp. 20-21)

The strategy for a good corporate cyber security risk management should clearly frame the cyber threats, in order to assure the fulfillment of cyber resilience organizational purposes.

A strong risk management plan must include:



An increased level of anticipation in terms of possible threats. Anticipation should lead to simulations, that should merge the corporate team into a brainstorming action of planning in order to efficiently control the damage of an eventual attack, and how to recover after a cyber attack.



Resistance plans are also a core element of a valuable corporate risk management plan, and it includes acknowledging eventual threats, but also acknowledging the required level of acceptance to some unrecoverable damages, or that some kinds of damage take time to fully recover, also there is required a system of mirroring, so that the threats and their desired effects are mirrored back to the sender; and last but not least, the acceptance of the fact that we should simply remove programmes that contain signs of an eventual threat.



Recovery plans should also be an important part of the whole plan, actions that include rebuilding, replacing and reconstitution in order to discover where exactly we should work on improving our cyber security methods and systems.



Adaptability is required in a corporate risk management plan, especially in terms of cyber security, all of the employees should take full responsibility and should acknowledge the requirements of a

strong cyber security system, and to adapt to the new terms and conditions of corporate functioning. (Ross, Pillitteri, Graubart, Bodrau, McQuaid, 2019, pp. 78 - 79)



4.3 Employee Training and Awareness Programs

Employee Training in Cyber Security

To assure a high level of adaptability of the employees within a cyber security risk management, within an organization, training in this area is often required, training which would help the corporate workers to understand the importance of this matter. (Ross, Pillitteri, Graubart, Bodrau, McQuaid, 2019, pp. 78-79)

Cyber Resilience Awareness Program

Building cyber resilience and security awareness in an organization is crucial to ensure the integrity of the company's data, as well as your employees'. Providing all employees with a basic understanding of cyber security will prevent lapses caused at an organizational level. It's important to be equipped with the necessary knowledge in the event of a cyber incident occurring, no matter the position within the company.

The objective of such a plan is to increase awareness and understanding of cybercrime, as well as teach employees how to identify and respond to it. A solid awareness program leads with fundamental information, such as a definition of cyber resilience and security, an outline of risks, followed by a rundown on cyber threats and vulnerabilities, as well as examples of recent cyber attacks (Christopher, Choo, & Dehghantanha, 2017). Employees have an easier time remembering real life examples and stories that pertain to cyber security, and they retain more information that impacts their behavior (Bagheri, Ridley, & Williams, 2023). This can be done through email newsletters, posters and brochures.

In order to increase awareness, it's necessary to create a sense of responsibility for security amongst employees and explain how their actions can put the organization at risk (Christopher, Choo, & Dehghantanha, 2017). With the handling of vital and private information, there is a need to assure that all devices are updated and secure, employees create strong passwords, use multi-factor authentication, etc. (Annarelli, Nonino, & Palombi, 2020). Employees will pay closer attention to practical advice, in which case a phishing simulation exercise could help them better understand why it's important to be cyber resilient and how their actions affect the organization.

Exchange information and report potential threats should also be encouraged. Establishing early warning signs and informing the stakeholders ensures the containment of the incident (Petrakos & Kotzanikolaou, 2019). Providing documentation and a reporting platform will aid in detecting future breaches and promote communication between employees (Christopher, Choo, & Deghantanha, 2017).

In the end, to guarantee the effectiveness of the program, test employee knowledge with quizzes and assessments. Keeping the program consistently refreshed and up to date is a necessity to protect the organization from contemporary and advancing cyber threats.



Case Study

Some examples of successful cybersecurity awareness programs include STOP. THINK. CONNECT. This global cybersecurity awareness effort promotes safe practices online, as well as encourages people to think more critically in regards to their online security. The campaign was launched in October of 2010 and since then it has expanded, involving governments, organizations, and individuals worldwide. With an emphasis on the shared responsibility of all parties in creating a safer online world, it aims to educate individuals about common cyber threats such as phishing, malware, identity theft, and social engineering.

Stop. Think. Connect. provides an extended range of resources to help everyone enhance their cybersecurity. These resources include tip sheets, videos, posters, social media content, and educational materials covering topics like password security, online privacy, mobile device safety, and safe social media usage.



4.4 Developing a Cyber Incident Response Plan

It's important not only to try preventing cyber incidents, but also to be prepared when they do eventually occur, as they are unavoidable. Organizations can take several steps and measures to avoid even bigger losses such as revenue loss,

brand damage and customers losing trust. An incident response plan typically contains reactive approaches, though proactive strategies are just as critical, to identify the threats ahead of time. Following the NIST Incident response plan, being proactive in such a scenario includes preparation, from employee training and awareness programs, to a risk assessment plan, and updating hardware and software. Reactive incident response refers in part to the detection and analysis of the threat, specifically precursors and indicators. This type of response also involves containment, eradication and recovery from the incident. After this has been achieved, the post-incident activity phase is in place, and the organization learns and prepares for the next inevitable incident. During this stage, evidence is gathered, recorded and managed, which is a crucial step, as it will speed up the process during future events like this (Shinde & Kulkarni, 2021).

During the detection and analysis process, it's of utmost importance to identify the list of risk priorities. This is necessary due to the extensiveness of the attack surface. It would be impractical to have countermeasures for every type of possible threat, as costs would be significant. In this case, the first step is determining which potential attacks warrant preventive measures and establish a perimeter containing only the risks with the highest priority (Annarelli, Nonino, & Palombi, 2020).

In a cyber incident response plan, each step, from preparation to post-incident, is dependent on the previous, so it is necessary to follow them in order (Kral, 2021).

In the end, a response plan should include policies and regulations, governance, information sharing, as well as mutual aid, coordinated action, and systemically, risk markets and embedded security.



4.5 Data Backup and Recovery Plan

Organizations require strong backup systems and recovery plans to ensure they can run smoothly despite compromised systems and data. The measures taken for backup and recovery allow for a quick and effective restoration of operations. A backup system is vital for business continuity, while a recovery plan is advised to have in case there is a possibility to retrieve important and private data that was lost during the cyber attack.

As a means for preparation for an incident, data has to be frequently backed up. Companies should have policies in place that state the regularity with which the backup will occur, in accordance with the existing data's nature and criticality, as well as the rate at which new information is added in. The backup policies need to include records for where the data is stored (NIST, 2012).

Keep in mind that depending on the level of impact, there are several ways to tackle a disruption and ensure a safe data backup.

In order to have fully functional and swift backup systems, organizations can start with data backup management. To prevent data loss in the case of certain incidents, like fire or theft, it is required to store backups in a separate location, distant from the central server equipment. Secondly, off-server copy management is recommended. This allows the organization to access necessary data for the recovery plan quicker. It can be done through the use of removable media, such as hard-drives, and physically transporting it to an off-site location. Additionally, storage device management is advised in order to organize the data. In this case, there are risks, like the media being damaged during transit. To avoid this, companies can opt for serverless copy management, which involves the use of a Virtual Private Network (VPN). This removes the necessity of physically moving the information, although the costs might be higher. It is of high importance to ensure that only authorized people have access to the location of the data and store it in a protected area, both of which can be done through encryption systems and nondisclosure agreements (Ramesh, Logeshwaran, & Aravindarajan, 2023).

A recovery plan refers to collecting the data that was backed up previously. Having a good recovery infrastructure is key to safely retrieving critical information. Depending on the nature of the backup system that is in place, the recovery can take up to a few days.

The recovery levels can be categorized in tiers, with two important measures: recovery time objective (RTO) and recovery point objective (RPO). They are necessary to assess the best solution based on cost considerations. RTO refers to the timeframe in which functions are not available and have to be restored. Its duration is dependent on the tasks required for restoration capabilities on the backup server, ranging from a few days to less than a minute. RPO is the timeframe between two consecutive backups, and refers to the loss limits once the restoration is seen as successful. It can take up to 24 hours depending on the system (Suguna, & Suhasini, 2014).

In short, the necessary steps to create a good backup system and recovery plan are:

- ✔ Identifying critical data and categorizing it based on importance and impact if lost.
- ✔ Assessing the requirements for safe backup for each category; Find appropriate backup storage locations and ensure their safety and accessibility.
- ✔ Select which backup solutions are suitable.
- ✔ Determine the procedure for backup and recovery, including how their integrity will be assessed.
- ✔ Implement automation through different tools.
- ✔ Prepare documentation for the process, from responsibilities, to procedures.
- ✔ Authorized employees that have access to the data should receive proper training.
- ✔ Regularly test the methods used for both backup and recovery.
- ✔ Review and update the backup systems and recovery plans according to needs, new technology and evolving threats.

CYBER RESILIENCE FROM A DAILY PERSPECTIVE



5.1 Identifying Vulnerabilities in Your Personal Life and Ways to Respond

When it comes to personal security and protection of data, we have seen tremendous growth in this sense. In this day and age where access to information is just a few clicks away, we have become power users, both of our devices and social media accounts. Therefore, if our devices and digital footprint are at risk of being compromised, so are we. The aim of this section is to empower you as users to take a closer look at your digital footprint and be more aware of your online habits. The following subsections touch upon the first step of your cyber resilience strategy: detection of vulnerabilities and protection against cyberthreats.

5.1.1 Personal Devices

The preliminary step most individuals take when it comes to the protection of their personal devices is virus related. This is why, for most people, their first instinct is to use an antivirus product from the hundreds already available on the market. While such tools might have proven useful in the past, they are rapidly losing their efficiency, and the statistics are deeply revealing. In December 2012, researchers from Imperva, a data security research firm in Redwood Shores, California, and students at the Technion–Israel Institute of Technology tested the antivirus tools by collecting 82 new computer viruses and running the malware against the threat-detection engines of some of the world's largest antivirus companies, including Microsoft, Symantec, McAfee, and Kaspersky Lab. The results showed that only 5 percent of the scanned threats were detected, meaning that 95 percent of the malware was not perceived as a threat. (Goodman, 2015, p. 20)

While antiviruses seem like a good idea, both creators of malware and the software companies themselves are evolving at different rates. Patches and updates from the antivirus software may come out months later with the threats themselves becoming more dangerous and undetectable, both to you and to the software you are using. On the other hand, what we know today as personal

devices is not limited to personal computers (PC's) but also to smartphones, smart TVs and tablets which are in comparison left exposed to any potential threats. Sadly, there are limited solutions available on the market to prevent the infection of these devices. The Apple device ecosystem is one key example of this issue, with virtually no built-in antivirus or malware detection software or any alternatives in the App Store.

5.1.2 Social Media

Social networks are the 21st century's public records. You may put at risk not just yourself but those connected with their social network too, simply by displaying personal or other sensitive information on their social media profile, often about your hobbies and interests, that may be easily accessible to the cyber criminals. Everything you share, willingly or not gets collected sorted and stored only to be sold to advertisers, governments, and third-party data brokers, each with an increasingly voracious appetite to know the most intimate details of your life. These data can be used to determine things such as health conditions, life insurance and other things of that nature which will get used by any of the Big Four (Google, Amazon, Meta and Apple). Google uses your searches to profile you for prospective advertisers and data miners who in turn feed you content based on your searches, regardless of the source of the content: e-mails, voice mails, photographs, videos, and locations as cataloged by Google.



Case Study

Just take the example of the Target scandal in which a Minneapolis man learned his daughter was pregnant from his local Target store who was sending the fifteen-year-old girl coupons for items that did not meet her father's approval. Target's algorithm worked its magic by aggregating a customer's entire purchase history with demographic statistics purchased from data brokers.

In total, Target was able to identify twenty-five products which created the "pregnancy prediction score" which identified pregnant women were identified before anyone else could make the connection. (Goodman, 2015, p. 69)



5.1.3 Account Management

- ✔ Assessing the requirements for safe backup for each category; Find appropriate backup storage locations and ensure their safety and accessibility.
- ✔ Select which backup solutions are suitable.
- ✔ Determine the procedure for backup and recovery, including how their integrity will be assessed.
- ✔ Implement automation through different tools.
- ✔ Prepare documentation for the process, from responsibilities, to procedures.
- ✔ Authorized employees that have access to the data should receive proper training.
- ✔ Regularly test the methods used for both backup and recovery.
- ✔ Review and update the backup systems and recovery plans according to needs, new technology and evolving threats.

5.1.4 Phishing and Social Engineering Hacks

While phishing was previously defined in chapter 4, subsections 4.1 and 4.2. In terms of preventing the possibility of becoming targets of phishing, keep these measures in mind:

Always check the spelling of the URLs in email links before you click or enter sensitive information. An official, trusted source will not have any typos in their URLs. While on the topic of URLs, pay attention to URL redirects: if you click a particular link, you may find yourself sent to a different website with an identical design.

If you receive an email from a known source, but the contents displayed in the email seem suspicious, do not reply, but contact them from a new email address, rather than automatically replying from your main email account.

Lastly, while it is highly tempting in this day and age to share everything about yourself on social media, keep your personal data to a minimum, avoiding giving out any details about your vacation plans, home address or your phone number. In case you are being a target of phishing via social media, think about these following questions:

- ✔ Do they have urgent demands for personal and sensitive information?
- ✔ Are they threatening to close or suspend your account?
- ✔ Did they alert you to a prize for winning something when you didn't enter any contest?
- ✔ Does the email demand that you take some action "immediately"?
- ✔ Do they have a questionable tone and unprecedented requests?
- ✔ Do they have grammatical errors and spelling mistakes?
- ✔ Do they have a suspicious signoff and greeting? (Lukic & Webster, 2020)

But how do you know you have been targeted? Be on the lookout for these signs:

- ✔ The contact arrives unexpectedly.
- ✔ Sender asks for something out of the ordinary.
- ✔ The requested action is potentially harmful.
- ✔ The attacker attaches an unusual file or URL.
- ✔ A sense of emergency is included.
- ✔ Responding to a question you didn't ask.
- ✔ Asking for immediate assistance.
- ✔ Asking you to donate to a charitable cause.
- ✔ Asking you to "verify" your information.
- ✔ Sending threatening or intimidating messages.

How about social media threats? Although phishing and social engineering fall under this category, the methods are not limited only to those but rather can also include:

- ✔ Fake news usually involving clickbait titles, disguised as malware.

- ✔ Likejacking or clickjacking – automated liking or accessing pages without your permission.
- ✔ Fake giveaways asking for your data to claim your prize as “winners”.
- ✔ Catfishing via dating apps – deceiving a potential target by setting up a fake dating profile.
- ✔ Fake friends or followers: some available through apps dedicated to gaining/buying followers.
- ✔ Identity theft or brand impersonation: identity theft refers to an individual whereas brand impersonation applies to companies.
- ✔ Private which include suspicious links. (Online Scams – 11 Social Media Threats and Scams to Watch Out for, 11 May)



5.2 Consistent Measures to Maintain Cyber Resilience in Your Personal Life

In today's interconnected world, maintaining cyber resilience has become more important than ever. With the rise of online threats we must take proactive measures to safeguard our personal information and protect ourselves against cyber threats. In this section we will explore various measures that you can take to maintain cyber resilience in your personal life, with a particular focus on measures related to personal devices, social media, account management, and phishing and social engineering hacks. By implementing these measures, you can better protect yourself against cyber threats and ensure that your personal information remains safe and secure.

5.2.1 Personal Devices

Personal devices, such as smartphones, laptops, and tablets, have become an essential part of our daily lives, allowing us to stay connected, work remotely, and access information from anywhere in the world. However, these devices are also a prime target for cyber threats such as malware, ransomware, and phishing attacks. In order to maintain your cyber resilience behavior on your personal device, you must take some consistent measures and make sure you stick to them. Here is a short list of measures that you can implement so that

you can enjoy the benefits of your personal devices while also keeping yourself safe and secure in the online world:



Use strong and unique passwords: Use strong passwords with a combination of letters, numbers, and special characters. Avoid using the same password for multiple accounts.



Enable two-factor authentication: Two-factor authentication adds an extra layer of security to your accounts and helps protect against unauthorized access.



Keep your software up to date: Regularly update your operating system, web browser, and all installed applications to ensure they have the latest security patches and bug fixes.



Use antivirus and antimalware software: Install reputable antivirus and antimalware software on your personal devices to protect against malware and viruses.



Back up your data: Regularly backup important files and data to an encrypted cloud storage service or an external hard drive.



Be cautious of suspicious links and emails: Avoid clicking on links or downloading attachments from unknown or suspicious sources, and be wary of unsolicited emails or messages.



Use a virtual private network (VPN): A VPN encrypts your internet traffic and helps protect your online privacy and security.



Use firewalls: A firewall is a security system that monitors and controls incoming and outgoing network traffic. Enable the firewall on your personal devices to protect against unauthorized access.

5.2.2 Social Media

Social media has become an important part of modern society, allowing us to connect with friends and family, stay up-to-date on current events, and share our experiences with the world. It has become a daily routine to scroll through our social media feeds in the morning, while we are drinking our coffee, or anytime we get bored. As social media platforms continue to grow in popularity, so do the associated risks of cyber threats such as identity theft, cyberbullying, and online harassment. To maintain cyber resilience in personal life, it is essential for you to take proactive measures to protect yourself on social media. To make it easier for you, here are some tips to help you secure your activity on social platforms:



Use strong and unique passwords: Use strong, unique passwords for your social media accounts and avoid using the same password across multiple platforms. This can help prevent unauthorized access to your accounts. Also, your password should be a combination of letters, numbers, and special characters.



Adjust your privacy settings: Take the time to review and adjust your privacy settings on each social media platform you use. This can help you control what information is visible to others and reduce the risk of identity theft or cyberbullying.



Avoid suspicious links and messages: Be wary of clicking on links or downloading attachments from suspicious sources on social media platforms, as these can be used to spread malware or steal your personal information. Do not respond to messages from shady accounts or, in case you know the sender, if the message contains information that you did not request. Always check with your sender if the content of the message doesn't align with your typical conversations.



Think before you share: Be cautious about the personal information you share on social media platforms, and think twice before sharing anything that could be used to steal your identity or compromise your safety.



Report any suspicious activity: If you notice any suspicious activity on your social media accounts, such as unauthorized access or changes to your account information, report it immediately to the platform's support team. Change your password and log out all of the devices.

5.2.3 Account management

A key aspect in maintaining cyber resilience in your personal life is effective account management, which involves managing passwords, protecting personal information, and staying vigilant against cyber threats. As previously mentioned, the rise of online threats such as identity theft and hacking, has made it mandatory for us to protect our online accounts at any cost. Some of the next measures that we are going to present have been previously stated, but we are going to roughly mention them just to make sure you don't forget about them.



Enable two-factor authentication: This type of authentication is an extra security measure that requires a second form of verification, such as a code sent to your phone, in addition to your password, and helps you protect your account against unauthorized access.



Keep software and apps up to date: Regularly update the software and apps on your devices to ensure that any security vulnerabilities are patched and to reduce the risk of cyber attacks.



Be cautious about third-party apps: Be careful when granting permissions to third-party apps that you connect to your accounts. Only grant the permissions that are necessary and avoid using third-party apps that ask for excessive permissions or are not from a trusted source.



Use a password manager: A password manager can help you create and store strong, unique passwords for your accounts, and can also help you keep track of them.



Monitor your accounts for suspicious activity: Regularly check your accounts for any unusual activity, such as unrecognized logins or changes to your account information, and report any suspicious activity to the platform's support team.

5.2.4 Phishing and Social Engineering Hacks

Phishing and social engineering attacks are some of the most frequent and dangerous cyber threats faced by individuals today. These attacks are designed to make you divulge sensitive information or take harmful actions, often through fake emails, websites, or phone calls. It is important to understand the gravity of phishing and social engineering attacks and what measures you need to take in order to avoid them.



5.3 Withstand: Reactions in Case of a Cybercrime

One of the most important aspects of cyber resilience is being able to withstand the initial shock of a cyber attack. In the event of a cybercrime, it is important to stay calm and take action.

Here are 4 steps that are important in case of a cyber attack:

1. Secure your device

Immediately disconnect from the internet and turn off your device.

WHY IS IT IMPORTANT? By disconnecting your device from the internet, you can prevent the attacker from continuing to access your device and any sensitive information stored on it. This gives you time to assess the situation and take steps to secure your device and prevent further damage.



2. Notify authorities

Report the incident to the relevant authorities, such as your internet service provider, bank, local law enforcement or cybercrime investigation agency.

WHY IS IT IMPORTANT? Reporting a cyber attack to the relevant authorities is an important step in protecting yourself and others from cybercrime and minimizing the impact of the attack.



National Cyber Security Website:

<https://dnsc.ro/contact>

National Cyber Security Call Center: 1911

3. Collect evidence

Gather any evidence related to the cyber attack, such as emails or screenshots, to aid in the investigation process.

WHY IS IT IMPORTANT? It's an important step in responding to a cyber attack because it can help you to identify the source of the attack, determine the extent of the damage, and provide evidence to support any legal claims.



4. Find support

It is essential to talk to someone you trust to help you manage the emotional impact of the incident and seek the support from specialists that can help recover from the attack such as IT specialists, your financial institution etc.

WHY IS IT IMPORTANT? Seeking support is an important step in responding to a cyber attack, as it can help you manage the emotional and psychological impact of the attack, provide you with the necessary resources and expertise to recover from the attack, and help to prevent further attacks in the future.



DID YOU KNOW?

One in seven cyber attacks are reported (DOJ statistics) this means 85% of cyberattacks remain hidden either due to shame or due to the lack of education on the matter.



5.4 Recovery and Adapt: Sharing Lessons Learned with Family and Social Circle

While recovering from a cyber attack can be challenging, it is possible to learn from the experience and become more resilient in the future.

Here are 4 tips on how to recover and adapt after a cyber attack:

1. Update your security measures

Ensure that your devices have the latest software updates and install antivirus and anti-malware software.

WHY IS IT IMPORTANT? Cyber attackers often exploit vulnerabilities in software and operating systems. Keeping your software up-to-date can help to patch these vulnerabilities and prevent further attacks. Installing antivirus and anti-malware software can also help to detect and remove any malicious software that may be present on your devices.



2. Change your passwords

Reset your passwords and use strong, and different passwords for your accounts that are difficult to guess.

WHY IS IT IMPORTANT? Changing your passwords is important because cyber attackers may have gained access to your accounts during the attack. By changing your passwords, you can prevent further unauthorized access to your accounts.



3. Educate yourself

Learn more about cybersecurity and stay informed about the latest cyber threats and trends.

WHY IS IT IMPORTANT? By educating yourself, you can become more aware of the risks and take steps to protect yourself, your devices and personal information. This helps in avoiding any possible future attacks.



4. Share your experience

Talk to your family, friends and social circle about your experience and share your lessons learned to help others avoid falling victim to cyber attacks.

WHY IS IT IMPORTANT? It can help raise awareness about the risks of cyber attacks. Sharing your experience can also help to reduce the stigma associated with cybercrime and encourage others to seek support if they experience a similar attack.



These are some of the imperative steps that help deal with a cyberattack and the aftermath. But keep in mind: prevention is always better than cure, so stay vigilant and stay safe online!

CONCLUSION

Having in mind the organizational landscape of the digitized world we live in, it is of paramount importance to develop a crisis management plan that puts emphasis on the role of communication, and on how firmly it can strengthen your cyber security system against compromise of data, reputation, money or visibility. Needless to say, people can become the target of cyber threats outside of a corporate scenario as well, by being targeted individually, which further proves how beneficial it is to value awareness and implement successful prevention. From this perspective, communication in crisis management does not come without its impediments: companies either lead by offering transparent communication to allow for full cooperation with everyone, or genuinely fail to communicate due to the fear of admitting their weaknesses when confronted with cyber attacks.

It all comes down to where we place this cyber crisis communication when we talk about being cyber-resilient. For that reason, this guide sheds light on the levels of communication triggered by different kind of attacks, on the ability of identifying your spokespeople and decision-makers, on understanding your stakeholders – who you should communicate with, what, when and how you should communicate – as well as paying attention to victims that are still vulnerable to additional attacks. The risk does not disappear after being exposed to a cyber attack, and it eventually becomes difficult to overcome it without a good cyber resilience strategy.

Cyber resilience functions through the power of listening and knowledge sharing, as well as efficient communication, aimed to provide a successful implementation of not only prevention of cyber crisis, but recovery plans as well. Under these circumstances, cyber resilience keeps an organization operational despite the occurrence of cyber security incidents, in a process that involves valuably applied frameworks and accurate maturity models.

The guide highlights cyber resilience as a collaborative effort which requires the involvement of every part of the organization, being employees and management or even other businesses the said organization works with, as well as cyber resilience knowledge for individual online activities. After all, there is a huge probability that, once your business partner is affected by cyber attacks, you are consequently threatened due to the large amount of information shared in your business partnerships.

We hope that, by carefully examining the information, users will grasp the notion of a “cyber-resilient digital native”, which does not only involve a vast and strong knowledge of cyber threats, but the ability to associate human reactions to resilience in the cyberspace and regularly practice self-examination of assets and weaknesses as well, following a good communication pattern. The guide we provided puts emphasis on cyber risks and cyber risk management, in a joint effort aimed at preventing unwanted consequences of cyber threats. Moreover, it explains the importance of being aware of both human weaknesses and technical vulnerabilities, as parts of a good cyber resilience strategy.

We live in a digitalized society, where we tend to increasingly expose ourselves online without paying it no mind. Matters that seem trivial at first, like sharing a contact or clicking on a certain page, become a huge impediment in keeping cyberspace safe. By analyzing multiple such cases of cyberspace ignorance, we conclude that disclosing too much information can be detrimental to cybersecurity and it is our responsibility to avoid such situations and raise awareness to possible digital dangers.

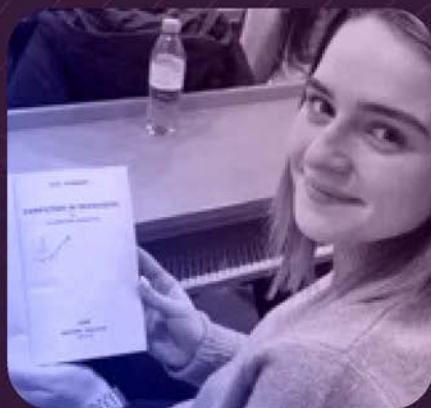
We are in need of a well-defined strategy in order to achieve a successful implementation of cyber resilience, built on a strong cyber security culture — a human firewall that aims at making safer choices on our multiple technologies, devices we use or digital services we relentlessly subscribe to. Any of us can become victims of cyber attacks at any given point in time, including organizations that follow a cyber resilience strategy and it is crucial to handle things carefully. Therefore, our level of awareness weighs on how much we can limit the damage of cyber threats.

The objectives of our guide are focused not only on providing a deeper understanding of the core concepts of cyber resilience but on the methods of prevention, preparation, response and recovery as well. For this particular reason, any introduction to cyber resilience requires a clear understanding of resilience itself, highlighting the cross-section between real world and cyberspace and how easy it is for any device to be compromised as we delve deeper into the development of any digitization process. Following the pattern of resilience, one can strengthen its progress through shared experience, by being aware of specific needs, threats, weaknesses and understanding that these skills are essential in both dimensions.

MEMORIES WALL

Student Clemența-Andreea Roșu:

The expert professors and practical approach helped me develop crucial skills in vulnerability assessment, penetration testing, and incident response. The emphasis on ethics and real-world experience made me a confident and responsible cyber security professional. I wholeheartedly recommend this course to anyone seeking a transformative education in the field. Prepare to empower yourself and make a real impact in the digital world.



Guest moment: Dragoș Ionică from Deloitte

I would like to share my experience as a presenter at the cyber resilience seminar for communicators and emphasize the importance of attending a well-structured course in this fascinating field. I had the privilege of being invited to deliver a presentation at this seminar, and it was an extraordinary experience. It was a unique opportunity to share my knowledge and experience in the field of cyber resilience with an interested and enthusiastic audience. I was impressed by the level of engagement and the participants' desire to better understand cyber threats and protective measures.

As a speaker, I was able to highlight the challenges and cyber risks that communicators face and provide practical solutions and strategies to overcome them. I encouraged participants to be proactive in managing cybersecurity, to assess their vulnerabilities, and to implement appropriate protection measures.

A valuable aspect of the seminar was the interaction with the audience. I had the opportunity to answer questions and discuss specific challenges that participants encountered regarding cybersecurity. This exchange of ideas and experiences added a practical and concrete dimension to the seminar and created an atmosphere of active and collaborative learning.

Attending this seminar further convinced me even more on the need to develop a specialized curriculum in the area of cyber resilience. I realized that the knowledge and skills required to be an effective communicator in the digital age cannot be ignored. It is essential to keep up with new technologies and understand the ever-changing cyber threats to provide accurate information and effectively manage communication in the event of incidents.

I highly recommend all communicators to participate in cyber resilience seminars and courses to strengthen their knowledge and develop their skills in this critical field. It is a valuable investment in their careers and in the ability to protect organizations from cyber threats.

In conclusion, I was honored to be a presenter at the cyber resilience seminar for communicators, and I am grateful to the organizers, Mihaela Pană, and Ms. Dean Alina Bârgăoanu for this opportunity. I confidently recommend attending similar events and continuing education in cyber resilience.



Guest moment: Andra Zaharia, cyber security communication specialist

Building cyber resilience gives you a unique advantage in the world:

- it strengthens your critical thinking and keeps you aware of the long-term results of your actions;
- it gives you the concepts and tools to operate with a clear head in a world shaped by technology;
- it helps you be comfortable with change because it gives you the confidence you can adapt to anything.

It also puts you in a position to help others, whether you're contributing to building businesses - others' or your own - or teaching people about the risks and opportunities in their environment.

Whichever adventure you choose, there's always something you can use from your cyber resilience toolkit.

Student Mădălina Manea:

Professor's dedication and expertise truly made a difference, creating an engaging and informative learning environment. The choice of well-prepared guests further enhanced the course by providing real-world perspectives and practical examples. I feel fortunate to have been a part of this course and am grateful for the professor's efforts in ensuring a positive and enriching learning environment.

Student Denisia Lupoi:

Through the program's rich tapestry of experiences, I discovered the immense power that lies within digital communication. It's not just about exchanging messages or sharing information; it's about creating meaningful connections, inspiring change, and leaving an indelible mark on the world. The program instilled in me the belief that my voice matters, and armed with the skills and knowledge acquired, I am now poised to make a real difference.



Student Ruxandra-Maria Chifan:

I highly recommend the Cyber Resilience course as it offers immense value for both our professional and personal spheres. The course material covers up-to-date information relevant to the present digital age and was directly applied in real-life scenarios. The teaching methods, course structure, and guest speakers collectively created a beneficial blend for us, the students aspiring to specialize in digital communication, and beyond.

Student Cătălina-Elena Albescu:

I'm happy that I have this chance to write about our Cyber Resilience course and to expose all the experience. It didn't feel like a normal/basic course, it was more like a free discussion combined with little games and interactive exercises. All the information that was given to us was up-to-date and well structured. It was easy for me to learn and to make connections with my professional life and what I need to do and not do. This experience opened my eyes and my curiosity in the cyber security area, and now, I want to know more about it.

Student Andrei Cristian Roșu:

The Cyber Resilience class was an invaluable experience that equipped me with the necessary knowledge and skills to protect against cyber threats. I feel confident in my ability to identify vulnerabilities, implement effective security measures, and respond to incidents. Highly recommended!

REFERENCES

AlEroud, A., & Karabatis, G. (2012). A contextual anomaly detection approach to discover zero-day attacks. 2012 International Conference on Cyber Security. doi.org/10.1109/CyberSecurity.2012.12

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers & Industrial Engineering. doi.org/10.1016/j.cie.2020.106829

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: management perspectives. Australasian Journal of Information Systems, p. 27. doi.org/10.3127/ajis.v27i0.4183

Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. IEEE Internet Computing, 10 (1), pp. 82–89. doi.org/10.1109/mic.2006.5

Christopher, L., Choo, K. K., & Dehghantanha, A. (2017). Honeypots for employee information security awareness and education training. Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, pp. 111–129. doi.org/10.1016/b978-0-12-805303-4.00008-3

Managing Insider Threats | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/managing-insider-threats>

Cybersecurity: main and emerging threats | News | European Parliament. (2023). <https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats>

Goodman, M. (2015). Future crimes: how our radical dependence on technology threatens us all. Doubleday Canada.

Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111 (7).

Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE international symposium on secure software engineering (Vol. 1, pp. 13-15). IEEE.

- Hruza, P., Sousek, R., & Szabo, S. (2014). Cyber-attacks and attack protection. In World Multi-Conference on Systemics (Vol. 18, pp. 170-174).
- Kaplan, J., Sharma, S., & Weinberg, A. (2011). Meeting the cybersecurity challenge. Digit. McKinsey.
- Kral, P. (2023). Incident Handler's Handbook | SANS Institute. www.sans.org/white-papers/33901
- Linkov, I., & Kott, A. (2008). Fundamental concepts of cyber resilience: introduction and overview. In Cyber Resilience of Systems and Networks. Springer. <https://arxiv.org/ftp/arxiv/papers/1806/1806.02852.pdf>
- Mandiant Unveils M-Trends 2023 Report, Delivering critical threat intelligence directly from the frontlines | Mandiant. (2023). Mandiant. <https://www.mandiant.com/company/press-releases/m-trends-2023>
- National Institute of Standards and Technology (NIST) (2012). Contingency planning guide for federal information systems. NIST Special Publication 800-34 Rev. 1. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>
- Petrakos, N., & Kotzanikolaou, P. (2019). Methodologies and strategies for critical infrastructure protection. In D. Gritzalis, M. Theocharidou, G. Stergiopolous (Eds.), Critical Infrastructure Security and Resilience, Advanced Sciences and Technologies for Security Applications (pp. 17-33). Springer.
- Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2023). A secured database monitoring method to improve data backup and recovery operations in cloud computing. BOHR International Journal of Computer Science, 2(1), pp. 1-7. doi:10.54646/bijcs.019
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). Developing cyber resilient systems: a systems security engineering approach (No. NIST Special Publication (SP) pp. 800-160. Vol. 2 (Draft)). National Institute of Standards and Technology.
- Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. Computer Fraud & Security, 2021(1), pp. 14-19. doi:10.1016/s1361-3723(21)00009-9
- Smith, E. A. (2005). Effects based operations. Applying network centric warfare in peace, crisis, and war. Command and Control Research Program (CCRP), Office of the Assistant Secretary of Defense, Washington DC.

Suguna, S., & Suhasini, A. (2014). Overview of data backup and disaster recovery in cloud. International Conference on Information Communication and Embedded Systems (ICICES2014).
doi:10.1109/icices.2014.7033804

The Human Factor Report 2022 – Threat Report | Proofpoint US. (2023, February 28). Proofpoint.
<https://www.proofpoint.com/us/resources/threat-reports/human-factor>

Threat Landscape. (2022). ENISA.
<https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends>

Ulsch, N. M. (2014). Cyber Threat! In Wiley eBooks.
<https://doi.org/10.1002/9781118915028>

Shields, K. (2015). Cybersecurity: Recognizing the risk and protecting against attacks. NC Banking Inst., p. 19, 345.

Hack the Hague 2021.
<https://illumeseecurity.co.uk/hack-the-hague-2021/>

Online resources:

Marr, B. (2021, July 2). The important difference between cybersecurity and cyber resilience (and why you need both) | Bernard Marr.
<https://bernardmarr.com/the-important-difference-between-cybersecurity-and-cyber-resilience-and-why-you-need-both/>

Resilience Services | Cybersecurity and Infrastructure Security Agency CISA. (2022).
<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services>

What is cyber resilience? | IBM. (2023).