Check Point
SOFTWARE TECHNOLOGIES LTD

form

CYBER ATTACK SECURITY GUIDE

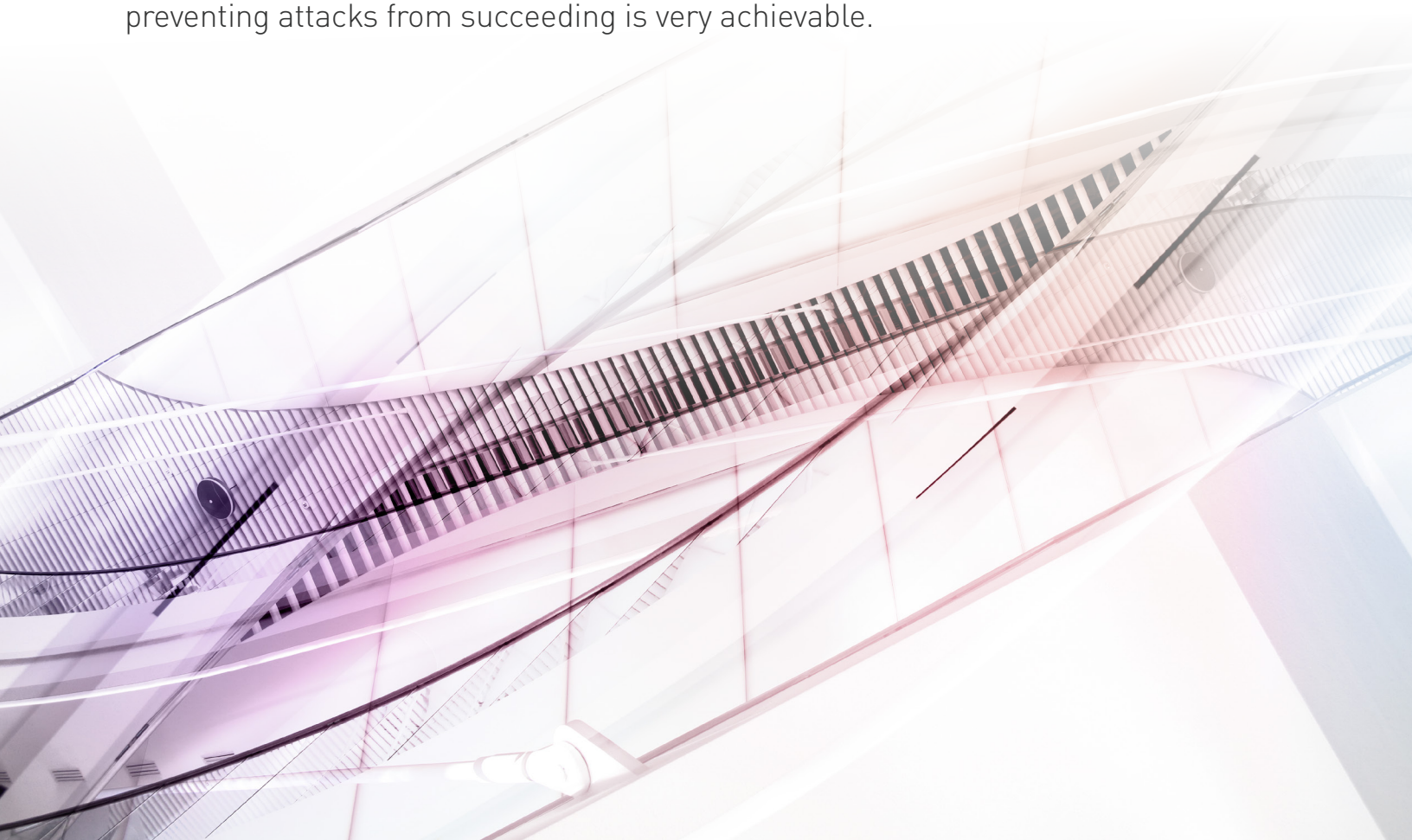
HOW TO PREPARE FOR FUTURE ATTACKS

BACKGROUND

New threats have become a weekly occurrence. Each week reveals innovative, advanced exploits that are threatening businesses and other organizations. These evolving security threats aren't a new phenomenon. As threats become more advanced, the impact of their damage also increases.

Hearing about cyber attacks in the news has become as common as reading about political events. In 2017 we have seen large-scale corporate breaches, state-sponsored attacks, U.S. intelligence leaks, and personal data compromised. While these attacks probably won't stop, they can be prevented by implementing cyber security solutions and proactive behavior.

This paper offers an overview of the attack vectors faced in today's world. It will guide you through the initial steps needed to prevent attacks and the immediate response protocol for containing attacks. While the potential for damage can be immense, preventing attacks from succeeding is very achievable.



OVERVIEW

Cyber attacks threaten everyone's daily lives. You don't need to be a politician or executive to become affected. Every infrastructure facility in today's modern world can become the target of an attack. Electricity transmission grids, banks, governments, automated homes, and even hospitals have become targets of cyber attacks.

Healthcare facilities hold extremely sensitive and critical information which could either save lives or cause bodily harm if patients' data is prevented from being accessed or even lost forever. There have already been attacks against hospitals which blocked vital records from being accessed, ambulances diverted, and in some cases entire departments shut down. Hackers are constantly creating destructive methods to overcome any security protection.

In addition to attacks against organizations, **nation-state** cyber attacks have become a new weapon in cyberwar. Government organizations issue nation-state weapons with the goal to disrupt or compromise. These weapons are leaking to cybercriminals who use them with malicious intent.

- **EternalBlue:** An exploit suite developed by the NSA which was leaked by the Shadow Brokers hacker group.
- **Vault 7:** WikiLeaks released over 8,000 documents and tools, belonging to the Central Intelligence Agency (CIA).
- **NotPetya:** Supposedly, Ukraine as a nation was targeted. The attack targeted banks, newspapers, electricity companies designed to cause maximum damage to organizations and temporarily cause them to be out of service.

Ransomware has gained in popularity among many homegrown attackers for the simplicity of buying Ransomware-as-a-Service (RaaS). It's easy for cybercriminals to monetize their activities with an affiliate ransomware service that provides ready-made command and control, and customer service for decrypting the data.

- **Cerber:** One of the most prevalent RaaS, offering the biggest affiliate program and adding innovative services like money laundering for cybercriminals.
- **WannaCry:** The attack spread and heavily disrupted the UK's National Health Service (NHS) and Spain's Telefónica, FedEx and Deutsche Bahn.

Just like computer vulnerabilities, **mobile vulnerabilities** can be executed via malicious applications, web-based or network attacks. Common threats include: promiscuous Wi-Fi, data leakage, spyware apps, and even phishing attacks over SMS.

- **Pegasus:** This spyware was capable of remotely hacking an iPhone and harvesting data about the victim using an implant. Once Apple deployed a quick fix, Pegasus reared its ugly head again with an Android version.
- **Viking Horde:** It created a botnet on rooted and non-rooted devices by using proxy IP addresses which disguised ad clicks. Every click generates revenue for the attacker.

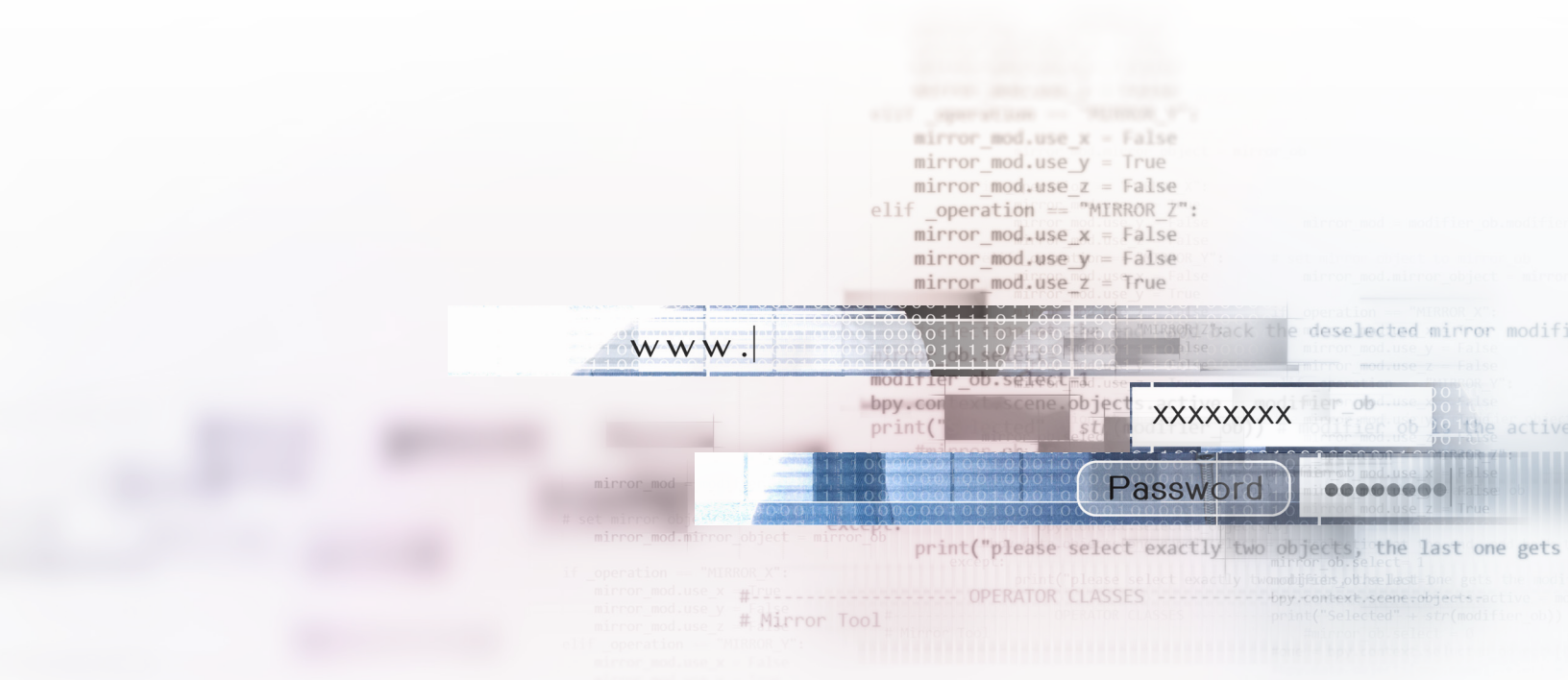
Data Breaches are nothing new, but as data is becoming more digitalized, the attack methods are also getting more advanced and dangerous. Private records are stolen and even government secrets are targets. But now, data breaches join with innovative monetizing methods that extort valuable information.

- **Equifax:** Due to an unfortunate breach caused by an Apache sever vulnerability; hackers were able to access Social Security Numbers, driver's license numbers, birth dates, addresses and credit card numbers.

- **Wells Fargo:** Human error, not a hacker, released troves of customer data. One of the bank's own lawyers accidentally leaked information linked to the bank's wealthiest customers.

Anyone can become a victim of a phishing attack. Victims will often receive an email from a spoofed account which is familiar to the target. Due to their low cost and the lack of user training, phishing attacks generally have a high success rate in compromising their target.

- **Tom Bossert:** An email prankster from the UK, disguised as Jared Kushner, emailed Homeland Security Adviser Tom Bossert about a "soiree," including a "personal email" to reach him.



5 STEPS TO PREVENT AN ATTACK

Getting victimized by a cyber attack isn't a predetermined fate. Attacks can be prevented despite the sophistication and overwhelming potential for damage.

So, what can organizations do to prevent an attack?

1 ASSESS YOUR RISKS

Think like a hacker and map your weak points. Start by assessing your risks and asking some of these important questions:

- What are your biggest threats (downtime, loss of data, exfiltration of data, vulnerable customer breach)?
- What are your crown jewels (reputation, data, service uptime, financial transactions, intellectual property, productivity)?
- Who are your enemies (competitors, nations, hacktivists, cybercriminals)?

2 LIMIT YOUR RISKS

Protect the perimeter and segment the internal network:

- Think of your internal network as lots of protected capsules. Start with offshore branch segmentation, than data centers, and move on to business units: financial, operational, customer support and R&D.
- Have different permissions and admins for each segment.
- Inspect the east west traffic moving between those units and protect the file shares.

- Allow auto-patching to unit groups which are not life supporting.
- Defend against attacks like Mimikatz which allow lateral movement by scrapping authentication hash from memory and using it to log into other work stations.

3 EDUCATE YOUR USERS

- Education is key.
- While it may not block every attack, it can prevent human errors and assist with the day-to-day maintenance of the IT surroundings.
- Educating users about suspicious activity in an effort to tip off your security team.

4 TEST YOUR DEFENSES

- Allow third parties to actively check if they can infiltrate the organization.
- "What if" test, and see how they can move inside of your network.

5 HAVE A RESPONSE PLAN READY IN CASE OF ATTACK

- Find "patient zero" and actively gather the logs and forensic data before you are breached.
- Allow remote quarantine of infection-spreading hosts.
- Be prepared with methods to actively search for infected users.
- Have response tools that can remediate new threats which were not blocked.

BOTTOM LINE

Cyber threats are evolving. In recent years, the growing number of threats has caused many organizations to face unfortunate repercussions. Cybercrime as an industry is only growing. With attacks and threats growing by the minute, so are preventative tactics to block these attacks.

To learn more, read this insightful paper on "How to prevent the next cyber attack".

Form IT Solutions

Premier Business Park, Dencora Way
Luton, Bedfordshire
LU3 3HP, United Kingdom

01582 572727
steven.mcallister@formits.com
www.formits.com

CONTACT US

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 |
Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-439 | 650-628-2000 | Fax: 650-654-4233 |

checkpoint.com