Aleksander Gorkowienko

Senior Managing Consultant
Spirent Communications

Agenda

Our meeting today

1. Hacking yesterday, today and tomorrow
2. Industries at risk
3. Cost of doing nothing
4. Mobile security
5. Security of IoT
6. Security of Industrial Systems (ICS/SCADA)
7. Telecommunication security (including 5G)
8. Automotive security
9. Medical security
10. How to secure your industry
11. Q&A

Introduction

Disclamer

- This course is for educational purposes only. It is intended to provide an insight into hacking for defensive purposes.
- This course is not an endorsement to undertake illegal or malicious activity in any form, unless such activity is properly authorised and you have obtained permission to do so.
- Spirent SecurityLabs takes no responsibility for any damage sustained to computer data, software or hardware through the use or misuse of tools referenced by this course.
- At the time of writing, Spirent SecurityLabs believes all information to be correct.
- Training material is (c) Spirent SecurityLabs and is for your own personal use only. The copying, recording, transcribing or photographing of any course materials, computer programs, computer code or digital information produced or supplied as part of any course is prohibited.

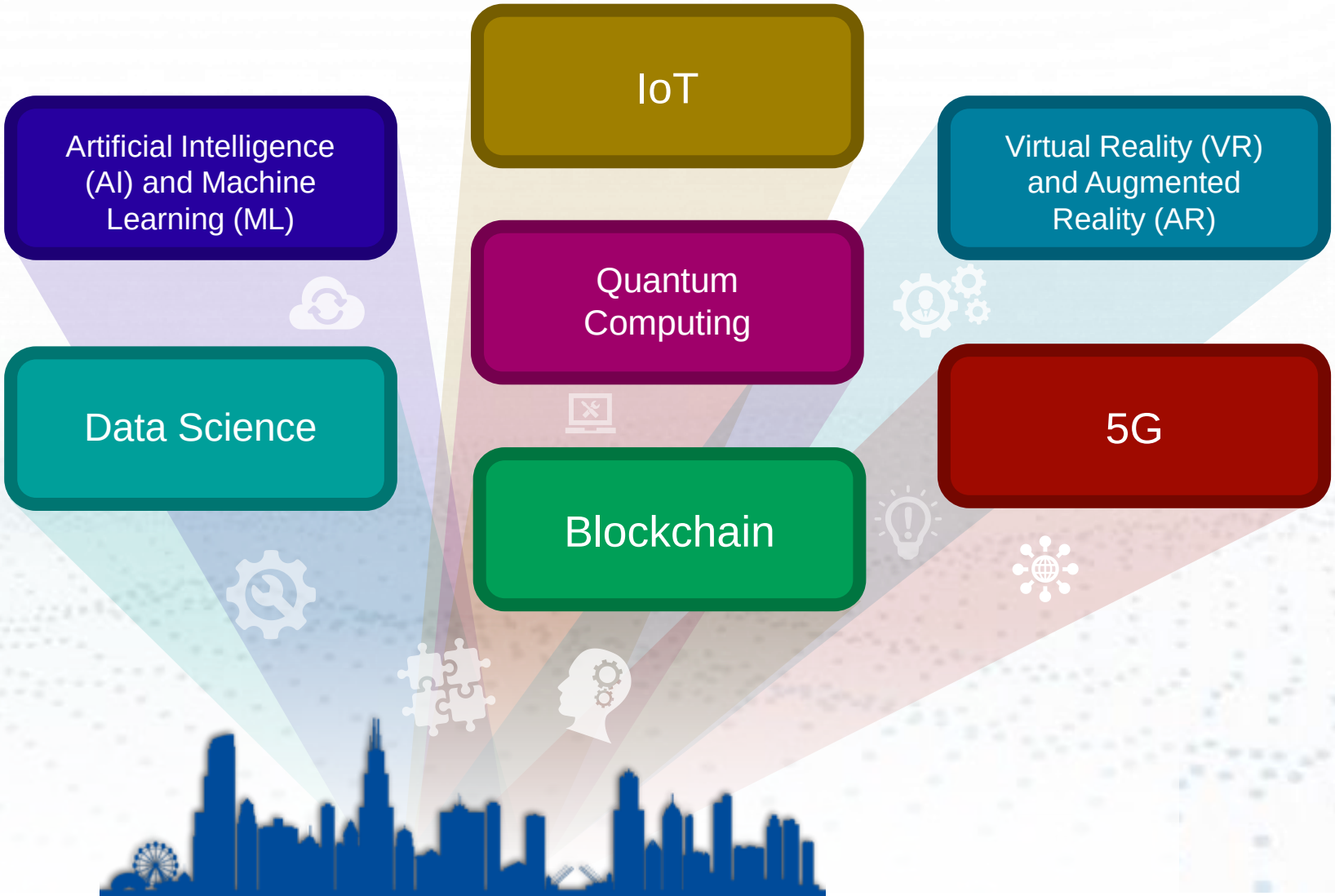
Stepping Into the Hacker's Shoes - Part One

Hacking yesterday, today and tomorrow

New technologies are already here so are the cybersecurity risks

New technologies have the power to impact the way we all live and work and truly shape our future.

None of these technologies is free from cybersecurity risks.



News are full of worrying articles about cybersecurity

spirent Promise. Assured.

82 percent of CIOs believe their software supply chains are vulnerable

By Ian Barker | Published 3 months ago

No Comments

HOSPITALS

Report: Increase in socially engineered, sophisticated cybersecurity attacks plagues organizations

A new report that showed a sharp increase

$43 billion stolen through Business Email Compromise since 2016, reports FBI

GRAHAM CLULEY FOLLOW @GCLULEY

MAY 5, 2022 | IT SECURITY AND DATA PRO

US eye clinic suffers data breach impacting 92,000 patients

July 2022 at 12:59 UTC

22 at 13:25 UTC

Healthcare US

ater Eye Center said customer data was involved in third-party cyber-attack

BRIAN BARRETT SECURITY AUG 18, 2021 2:59 PM

The T-Mobile Breach Is Much Worse Than It Had to Be

The vast majority of victims weren't even T-Mobile customers. Now their information is for sale on the dark web.

Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds

May 10, 2022

David E. Sanger and Kate Conger

23 FEB 2021 NEWS

84% of CNI Orgs Experienced Cyber-Attacks in the Last Year

James Coker Deputy Editor, Infosecurity Magazine

Follow @ReporterCoker

Related to This Story

UK prime minister's office smartphones targeted by Pegasus spyware

uncovered cyberattacks using Pegasus

and the Foreign and Commonwealth Of

Attacks/Breaches | 4 MIN READ | NEWS

Businesses Suffered 50% More Cyberattack Attempts per Week in 2021

The rise — partly due to Log4j — helped boost cyberattack attempts to an all-time high in Q4 2021, new data shows.

Hackers Can Clone Millions of Toyota, Hyundai, and Kia Keys

Encryption flaws in a common anti-theft feature expose vehicles from major manufacturers.

Industries at risk

Targeted industries

Top 10 industries targeted 2019 vs. 2020

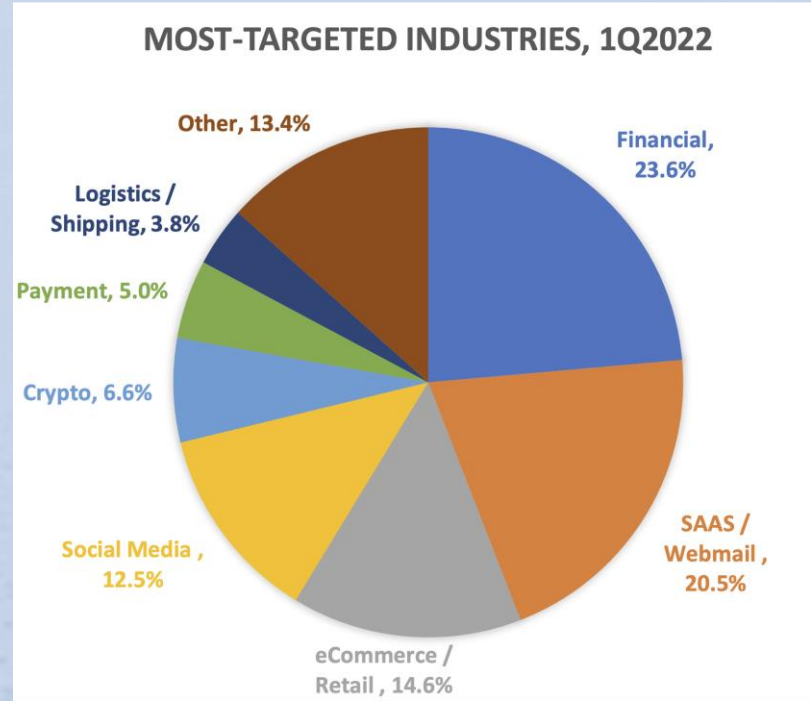
Top 10 industries ranked by attack volume, 2020 vs. 2019 | Source: IBM Security X-Force

Sector	2020 rank	2019 rank	Change
Finance and insurance	1	1	-
Manufacturing	2	8	6
Energy	3	9	6
Retail	4	2	-2
Professional services	5	5	-
Government	6	6	-
Healthcare	7	10	3
Media	8	4	-4
Transportation	9	3	-6
Education	10	7	-3

IBM Security / © 2021 IBM Corporation

Source: IBM 2021

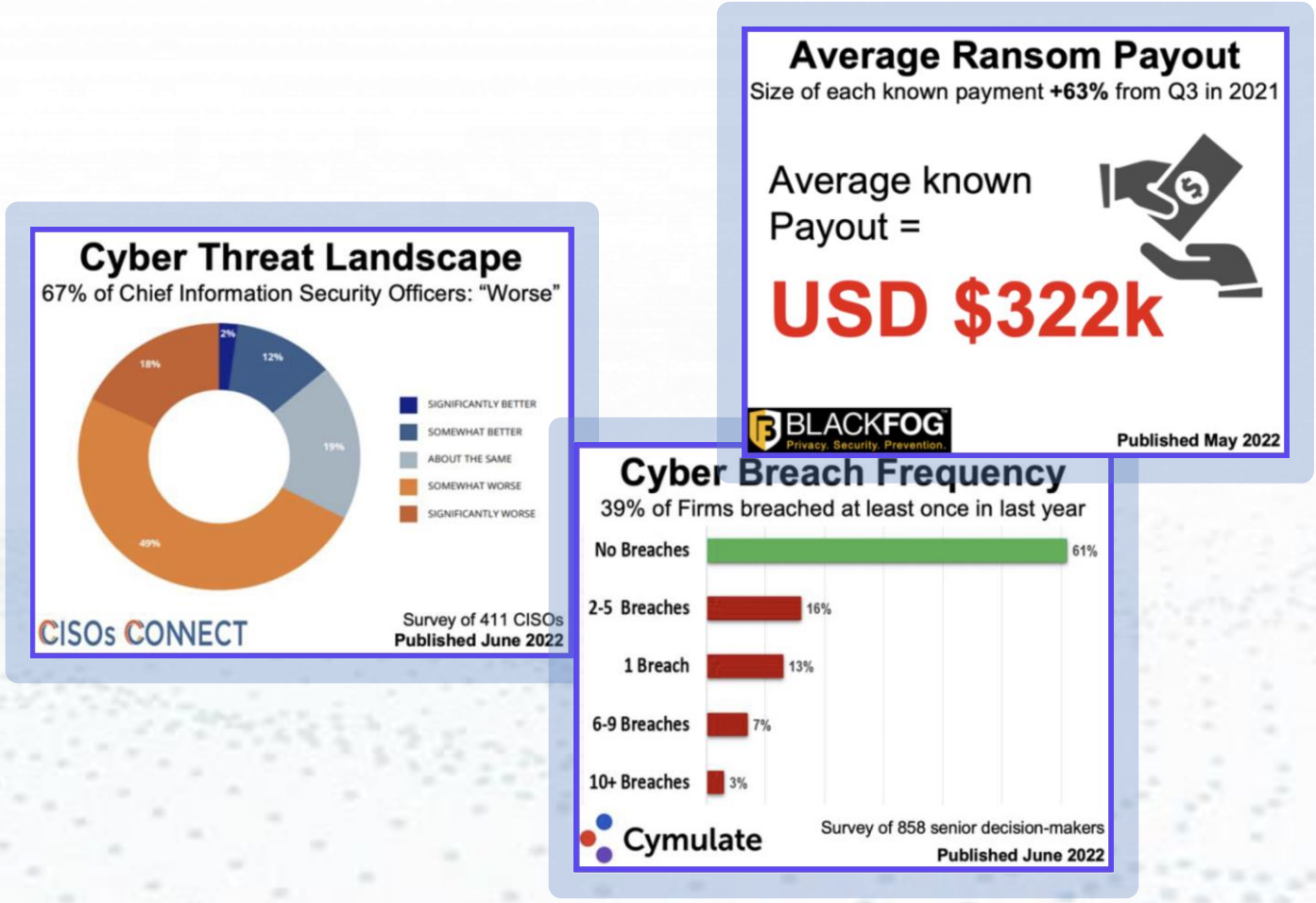
Industries targeted for phishing



Source: Anti Phishing Working Group 2022
(https://www.antiphishing.org)

Cost of doing nothing

You would still pay if you do nothing about cybersecurity.
Actually, you might pay more than you think…



Approach to cybersecurity

Reactive

- React **only after security breach** occurs
- Hoping the incident “never happens to me”
- Not knowing the security and performance posture
- Costs of recovering from attacks much greater comparing to proactive security approach

Proactive

- Focus on **preventing security issues** in advance
- Test security in lab
- Regular tests of live systems
- Detect security vulnerabilities
- Act accordingly on findings
- Improve security and processes
- Much less expensive compared to being reactive

Why CISO thinks his company is “secure”?

- …”because we bought a new firewall NG in January and it protects us so well”…
- …”because we have already invested £30000 to cybersecurity last year and we never had a single incident”…
- ...”because we control all the inbound traffic and have an antivirus installed”…
- ...”because our business does not attract hackers”…
- …”because our infrastructure is in the cloud so it is very secure”…
- …”because we conducted penetration test last year”…
- …”because we recently passed a compliance audit”…

THIS IS ALL **WRONG!**

Financial and insurance

Why financial services?
Well, because it is all about money!

What attackers are after?
Your money, of course. They might not necessarily grab all your money at once, but rather execute multiple micro transactions on your behalf. Your account can be used for unauthorised or illegal payments and you would not know about it.

Typical attack vectors:
Weak/stolen credentials, phishing email, malicious mobile app stealing your data.

Top protective controls:
Do not re-use credentials, use MFA, always manually log out from the banking website you've finished using, learn how to recognize phishing emails, compliance with the industry requirements, do not do multiple thing in your laptop/phone when using internet banking.

Telecommunication security (including 5G)

Why telecommunication?
All our data this or that way go through the telecommunication systems.

What attackers are after?
All type of sensitive and personal data (individuals and businesses), metadata, DoS.

Typical attack vectors:
Misconfigured and unpatched devices (on the provider side and on the customer side), known vulnerability (e.g., zero day), weak/default credentials, lack of network segmentation, malicious insider, supply chain threat, insecure IoT.

Top protective controls:
Have hardware devices patched and properly configured, have the devices security tested (ideally by unbiased 3rd party), network segmentation, security awareness training for personnel, compliance with the industry requirements, rigorous control of the supply chain, control system access.

Security of IoT

Why IoT?
IoT devices are the least secure from all. Typically they are a part of the internal network (home or corporate) so, if compromised, they can be a door to the network and everything in it. Quite often IoT devices are very cheap, forgotten by the vendor and never patched.

What attackers are after?
IoT devices are of a low value to attackers (unless they are wearables), so they rather used for pivoted attacks, using IoT devices as a part of botnet.

Typical attack vectors:
Misconfigured and unpatched IoT device, known vulnerability (e.g., zero day), “insecure by design”, weak credentials.

Top protective controls:
Use IoT devices from reputable vendors, have IoT device patched and properly configured, have IoT devices in a separate network segment. Bonus tip: reduce the number of IoT devices in your house. Not everything should be controlled by Alexa. ;-)

Mobile security

Why mobile devices?
Mobile phone is always on. All our life with all details: interests, pictures, passwords, secrets – all is there.

What attackers are after?
Literally everything which is on your phone (email, calls, chat history, personal data, credentials, geolocation, metadata – all can be monetized by hackers).

Typical attack vectors:
Weak/stolen credentials, malicious mobile app that is stealing our data, clicking the wrong link (especially in hybrid apps), app “insecure by design”, weak cryptography, insecure 3rd party components.

Top protective controls:
Do not re-use credentials, use MFA, do not install unverified apps, automatically update your phone and apps, always log out from the website you’ve finished using, do not download suspicious files, learn how to recognize phishing emails.

Security of Industrial Systems (ICS/SCADA)

Why ICS/SCADA?
ICS/SCADA devices are used by CNI, manufacturing and manage pretty much all industrial processes these days. ICS devices are well-known for being notoriously insecure as typically they operate in an air-gapped environment (which is not always the case).

What attackers are after?
Unauthorised access, DoS, takeover control of an industrial process, steal sensitive operational data, in consequence: blackmailing, ransom, etc.

Typical attack vectors:
Old, misconfigured and unpatched ICS device, known vulnerability (e.g., zero day), weak/default credentials, malicious insider, vulnerable USB drive, supply chain threat, insecure industrial IoT.

Top protective controls:
Have ICS device patched and properly configured, have ICS devices security tested, do network segmentation, security awareness training for personnel, compliance with the industry requirements, rigorous control of the supply chain, control system access.

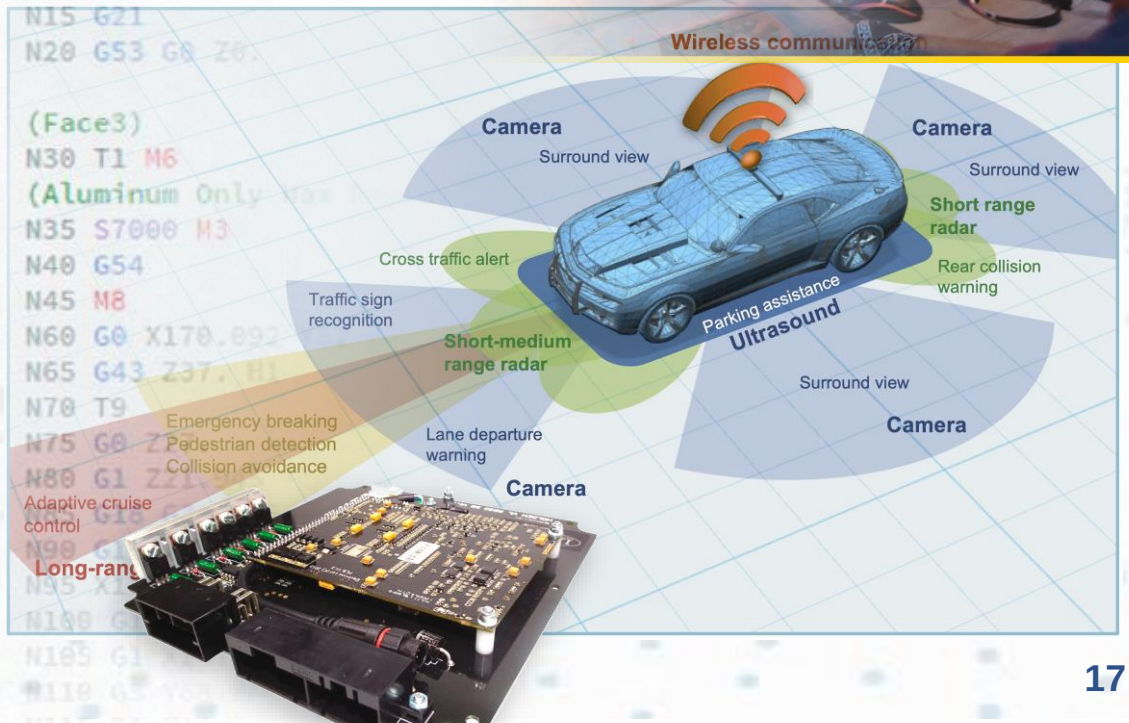
Automotive security

Why cars?
Modern cars have tons of electronic components, they are connected to the automotive cloud and can be managed remotely. Isn't it cool to start/stop someone else's car?

What attackers are after?
All type of sensitive and personal data, technical parameters of the car, geolocation (e.g., so they know you are not at home). The cherry on the top would be stealing your car or stopping it in the middle of the highway.

Typical attack vectors:
Insecure car components (e.g., infotainment system, ECUs), known vulnerability (e.g., zero day), weak/default credentials, malicious "insider" (in the garage), "backdoor by design", supply chain threat.

Top protective controls:
Have your car reviewed by an authorised dealer, do not do your own modifications in the car, control supply chain, rigorous control of the supply chain, compliance with the industry requirements. Bonus tip: consider using bicycle. ;-)



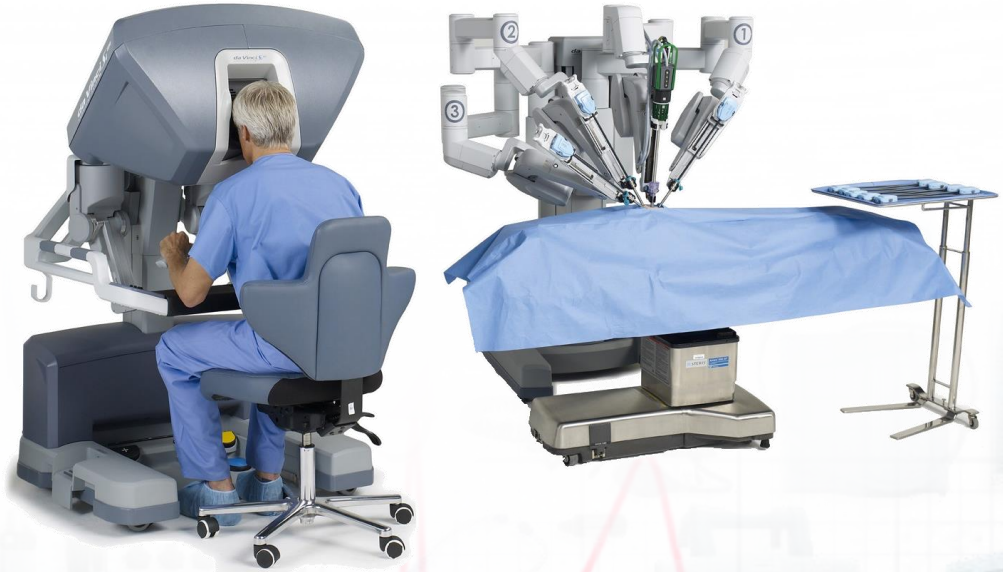
Medical security

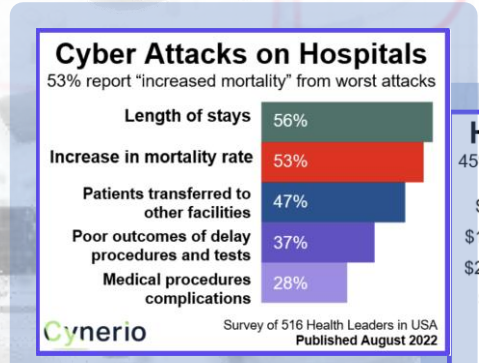
Why healthcare systems?
Modern medical systems feature the abundance of electronic devices and subsystems, they also use digital medical records (DMR). This data can be stolen and sold and devices circumvented.

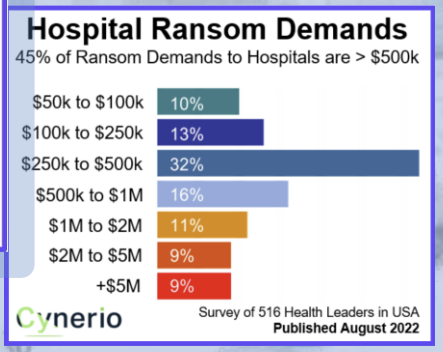
What attackers are after?
Digital medical records (DMR), parameters of medical equipment, taking remote control of the equipment.

Typical attack vectors:
Insecure/malicious mobile app, weak/stolen credentials, phishing email, known vulnerability (e.g., zero day), supply chain threat.

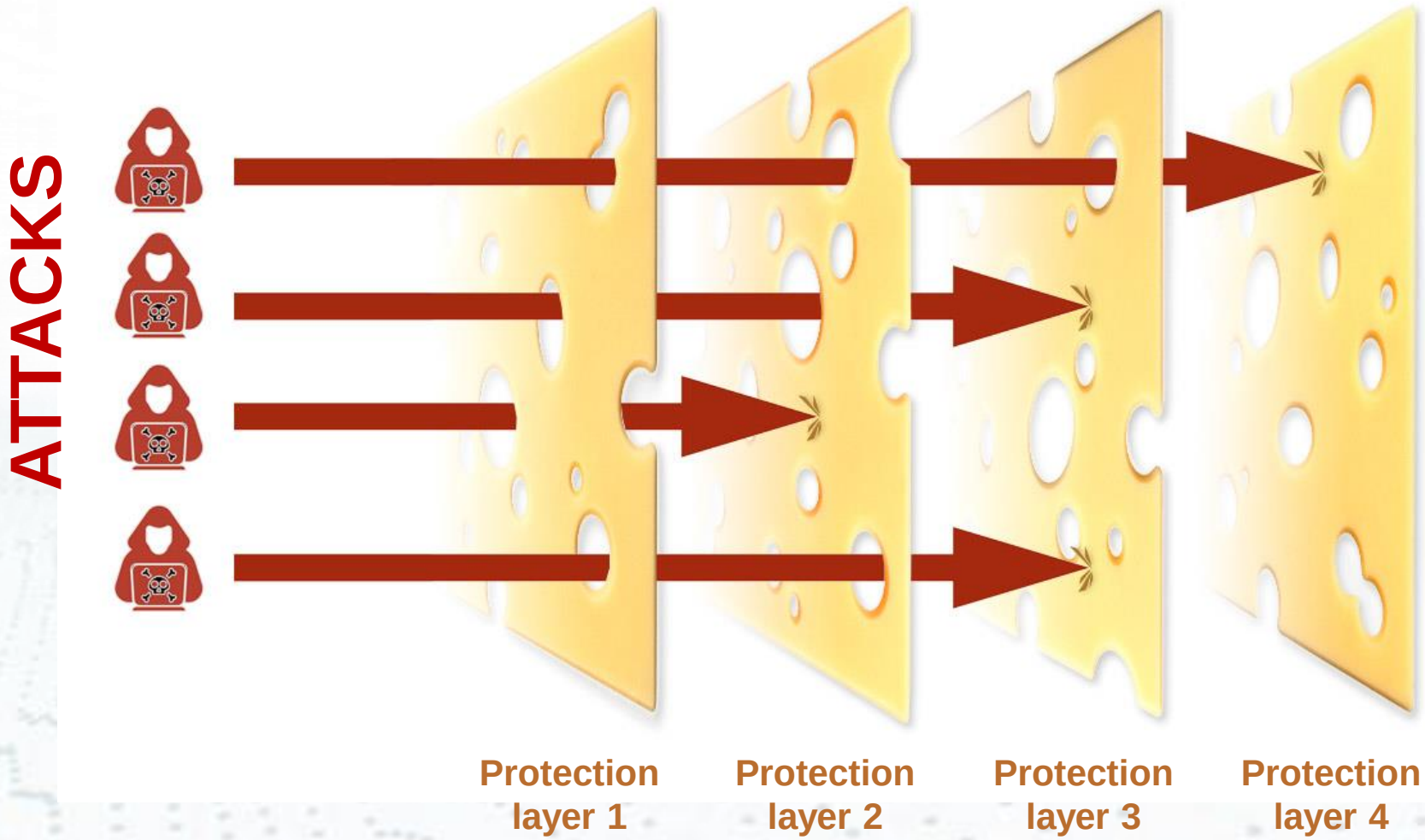
Top protective controls:
Keep software and OS up to date and patched, security awareness training for personnel, use trusted equipment vendors, rigorous control of the supply chain, control system access, compliance with the industry requirements. Bonus tip: stay healthy and avoid doctors. ;-)

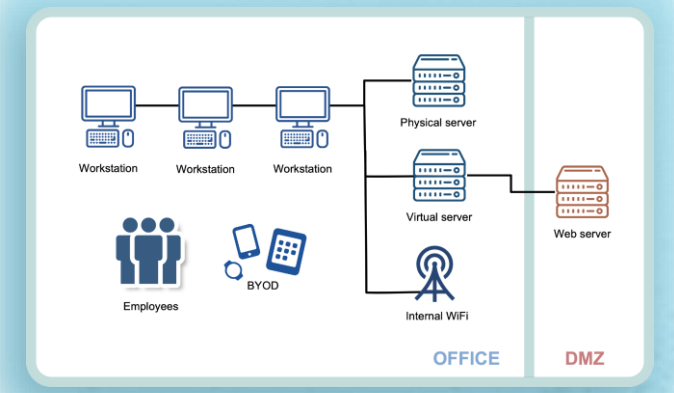






Takeaways: defense in depth





Your organisation

Takeaways: how to secure your industry

Generic protective controls for businesses:

- Map the network
- Identify all your IT assets
- Identify critical systems
- Reduce the attack surface
- Patch and update
- Keep software and OS up to date and patched
- Run security awareness training for personnel
- Use trusted equipment vendors
- Control of the supply chain
- Control system access
- Be compliant with the industry requirements
- **Conduct regular security assessments** (penetration testing) exercises
- **Never "assume" security. Always have it tested!**

All industries are different. Always learn and stay up-to-date with what is specific to yours.

Questions


WHEN? WHY? WHEN? WHERE?
WHAT? HOW? WHY? WHO?
WHEN? WHAT? WHERE?
WHO? HOW? WHEN?
HOW? WHERE? WHEN?
WHICH? WHEN? WHERE?
HOW? WHO?
WHAT? HOW? WHY?
WHY? HOW?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHY? HOW? WHERE?
WHO? WHOSE?
WHERE? WHAT? HOW?
WHAT? WHO?
WHERE? WHAT? HOW?
WHERE? HOW? WHERE?
HOW? WHO?
WHO? WHERE? WHAT? HOW?
WHAT? HOW? WHY?
HOW?

Thank you!

https://www.spirent.com/Products/SecurityLabs

securityLabs@spirent.com

securitylabs

Aleksander Gorkowienko
e: aleksander.gorkowienko@spirent.com
m: +44 (0) 7974431025