inetum.
realdolmen
Positive digital flow

"La Cybersecurité, une vaccination pour votre environment digital"
General program introduction

Program overview

1 **Security market watch "Understanding the trends, challenges & threats"**

Goal: Understanding the challenges and risks you face by clarifying and becoming aware of the impact and likelihood of threats

By: Inetum-Realdolmen – Thomas Tardieux

2 **Security vision "How to navigate your security transformation"**

Goal: Gaining practical insights in how you can approach your digital security transformation journey to improve your security posture and support the hospital business objectives

By: Inetum-Realdolmen – Thomas Tardieux

3 **Achieving adequate cybersecurity in Healthcare with Microsoft technology**

Goal: Gaining insights in achieving adequate cybersecurity in healthcare

By: Microsoft – Jonathan Jacqmin & Nadia Aime

inetum.
realdolmen
Positive digital flow

Security market watch
Understanding trends, challenges & threats

Content

01

Healthcare industry statistics

Data breach cost on the rise, highest in healthcare industry

inetum.
realdolmen
Positive digital flow

11

Consecutive years **healthcare** had the **highest industry cost** of a breach

Healthcare organizations experienced the highest average cost of a data breach, for the eleventh year in a row

93%

93% of the healthcare organizations experienced a **data breach the past 3 years**

57%

57% of the healthcare organizations experienced **more than 5 breaches** the past 3 years

30%

30% of all data breaches and data security incidents in the industry were **experienced by Hospitals**

6

Source: https://www.safetydetectives.com
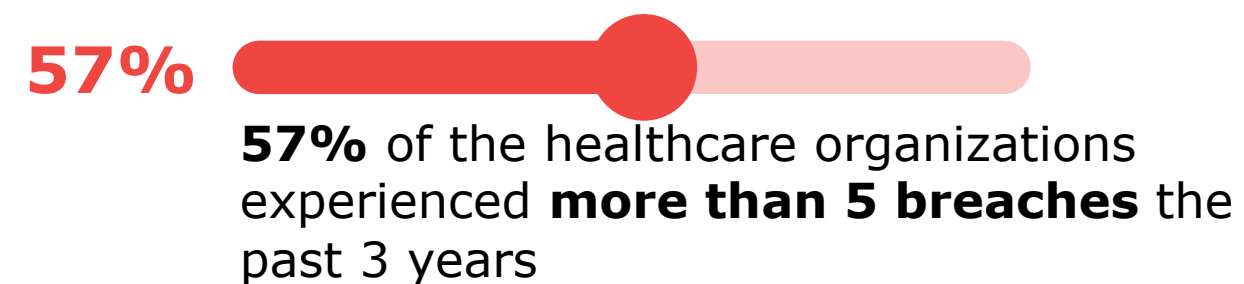
Data breach cost on the rise, highest in healthcare industry

Average cost of a data breach (measured in US$ millions)

Healthcare $9.23 $7.13

10%

Increase in average total cost of a breach, 2020-2021

The average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years
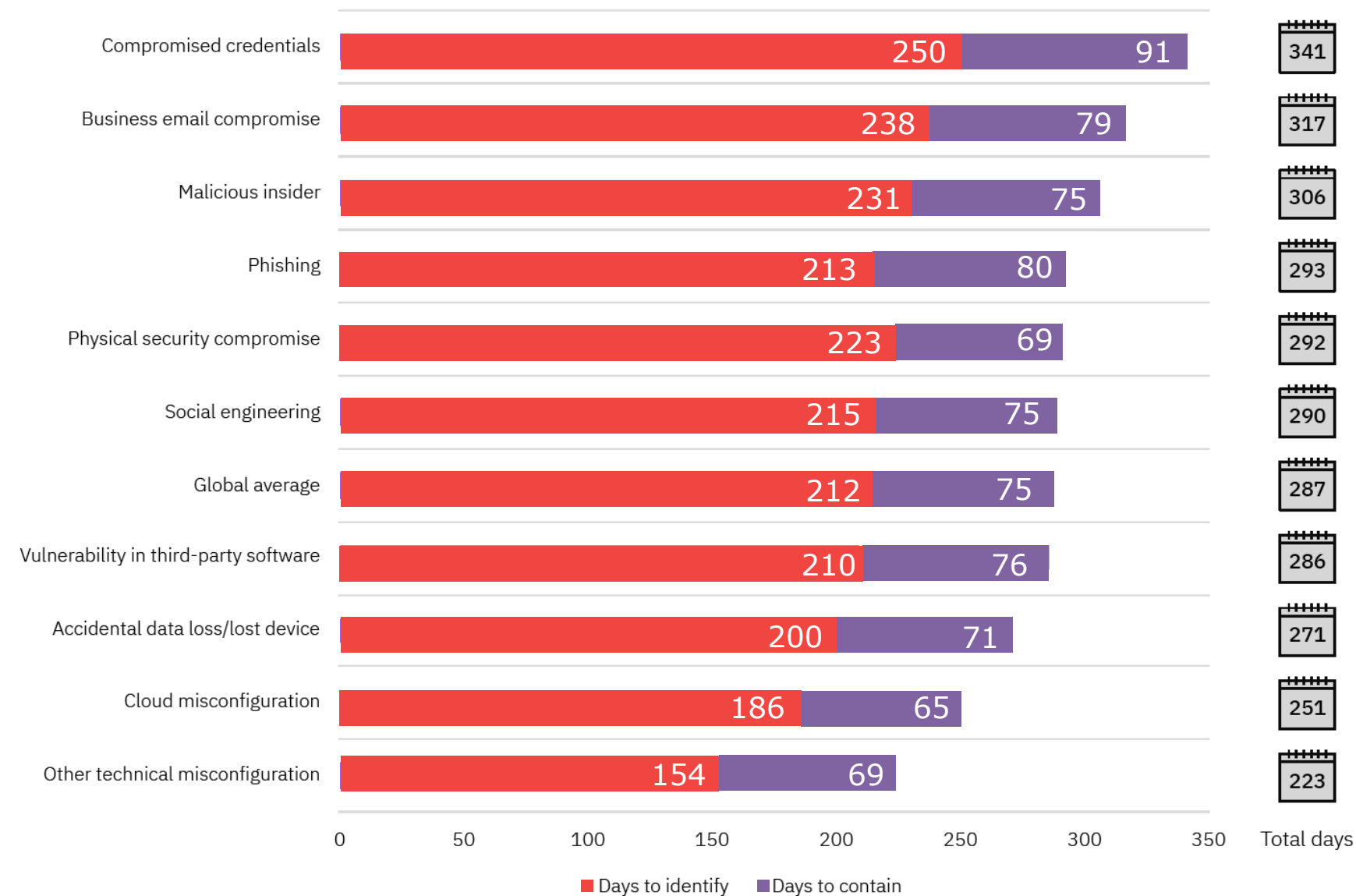
Industry	2021	2020
Healthcare	$9.23	$7.13
Financial	$5.72	$5.85
Pharmaceuticals	$5.04	$5.06
Technology	$4.88	$5.04
Energy	$4.65	$6.39
Services	$4.65	$4.23
Industrial	$4.24	$4.99
Global average	$4.24	$3.86
Entertainment	$3.80	
Education	$3.79	$3.90
Transportation	$3.75	$3.58
Consumer	$3.70	$2.59
Communications	$3.62	$3.01
Research	$3.60	$1.53
Retail	$3.27	$2.01
Media	$3.17	$1.65
Hospitality	$3.03	$1.72
Public sector	$1.93	$1.08

$0.00 $1.00 $2.00 $3.00 $4.00 $5.00 $6.00 $7.00 $8.00 $9.00 $10.00

■ 2021 ■ 2020

Source: IBM Breach Report

7

Average time to identify & contain the data breach

## Average time to identify and contain a breach by initial attack vector
Measured in days

Attack vector	Days to identify	Days to contain	Total days
Compromised credentials	250	91	341
Business email compromise	238	79	317
Malicious insider	231	75	306
Phishing	213	80	293
Physical security compromise	223	69	292
Social engineering	215	75	290
Global average	212	75	287
Vulnerability in third-party software	210	76	286
Accidental data loss/lost device	200	71	271
Cloud misconfiguration	186	65	251
Other technical misconfiguration	154	69	223

■ Days to identify ■ Days to contain

Source: IBM Breach Report

Theft or loss due to data breaches

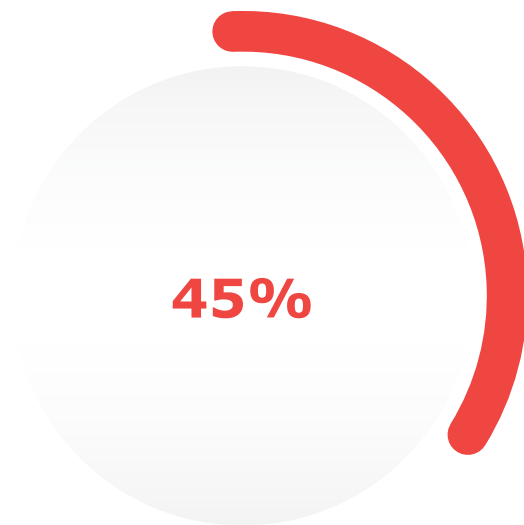Healthcare vs other industries

32%

Healthcare industry

15%

Other industries
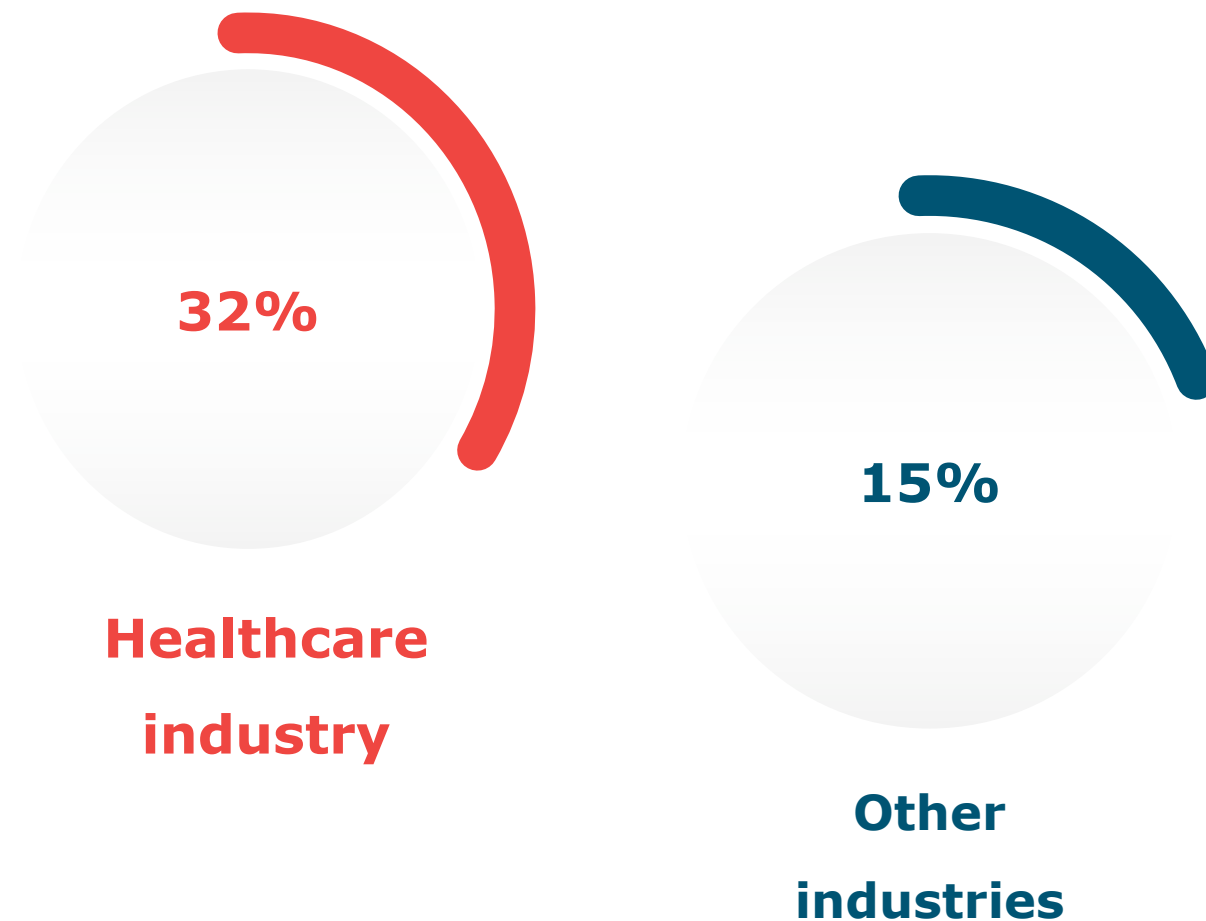
Medical records of patients sell for **$250** on average and go **up to $ 1.000** on the dark web. The are very valuable due to the amount of sensitive data that cannot easily be changed by victims

Overall increase of cyberattacks, especially in healthcare industry

Increased rates in cyberattacks from 10/2020 till 01/2021

45%

Increase of cyberattacks in healthcare industry

22%
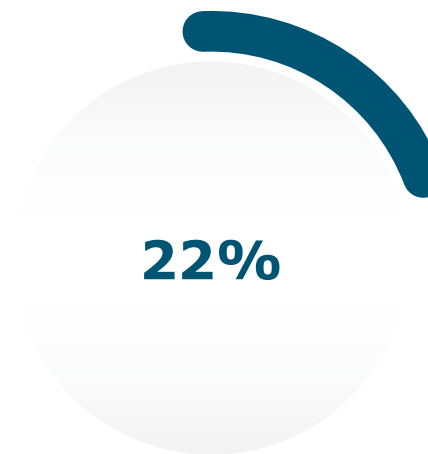
Increase of cyberattacks in other industries

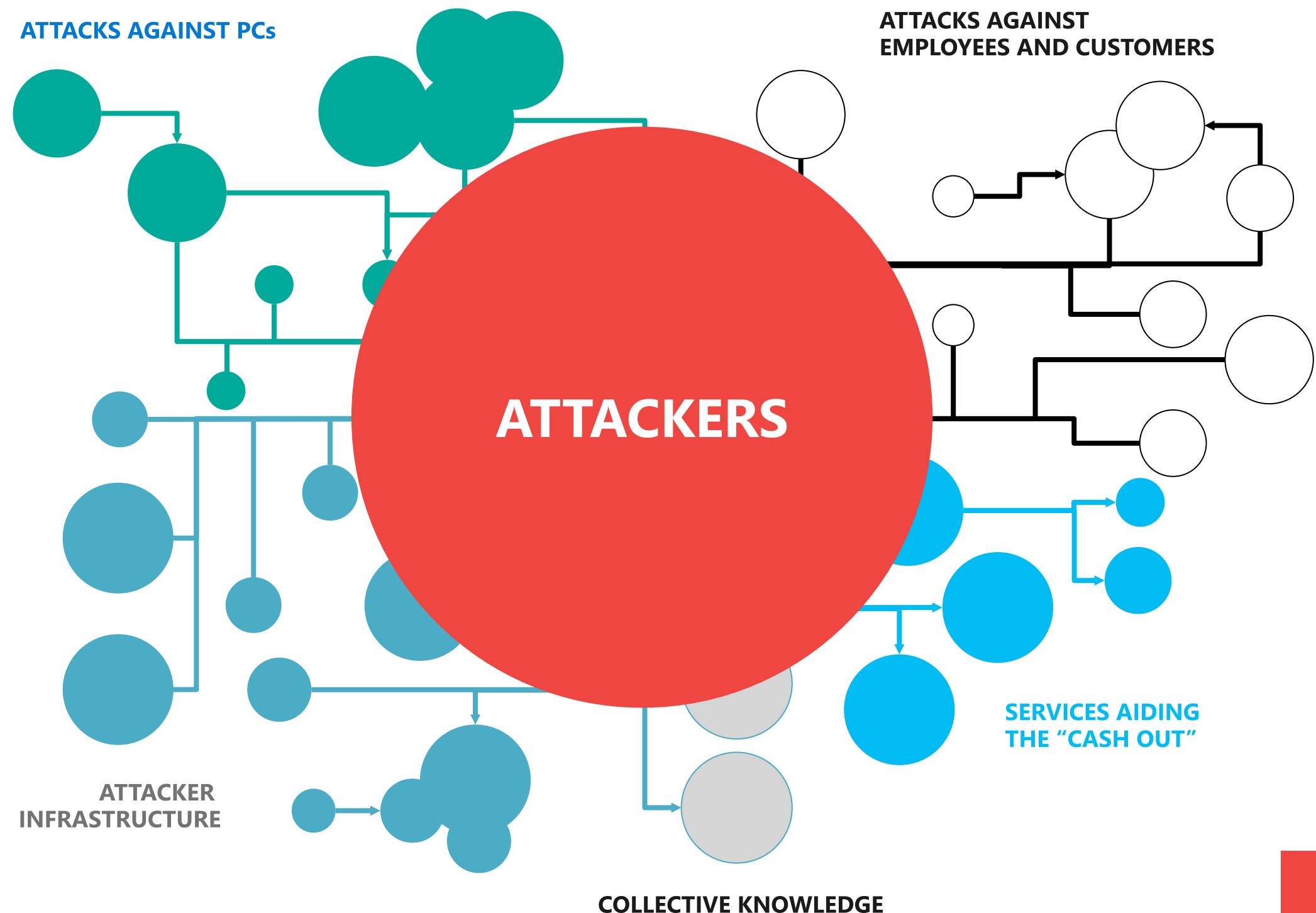Source: https://www.safetydetectives.com
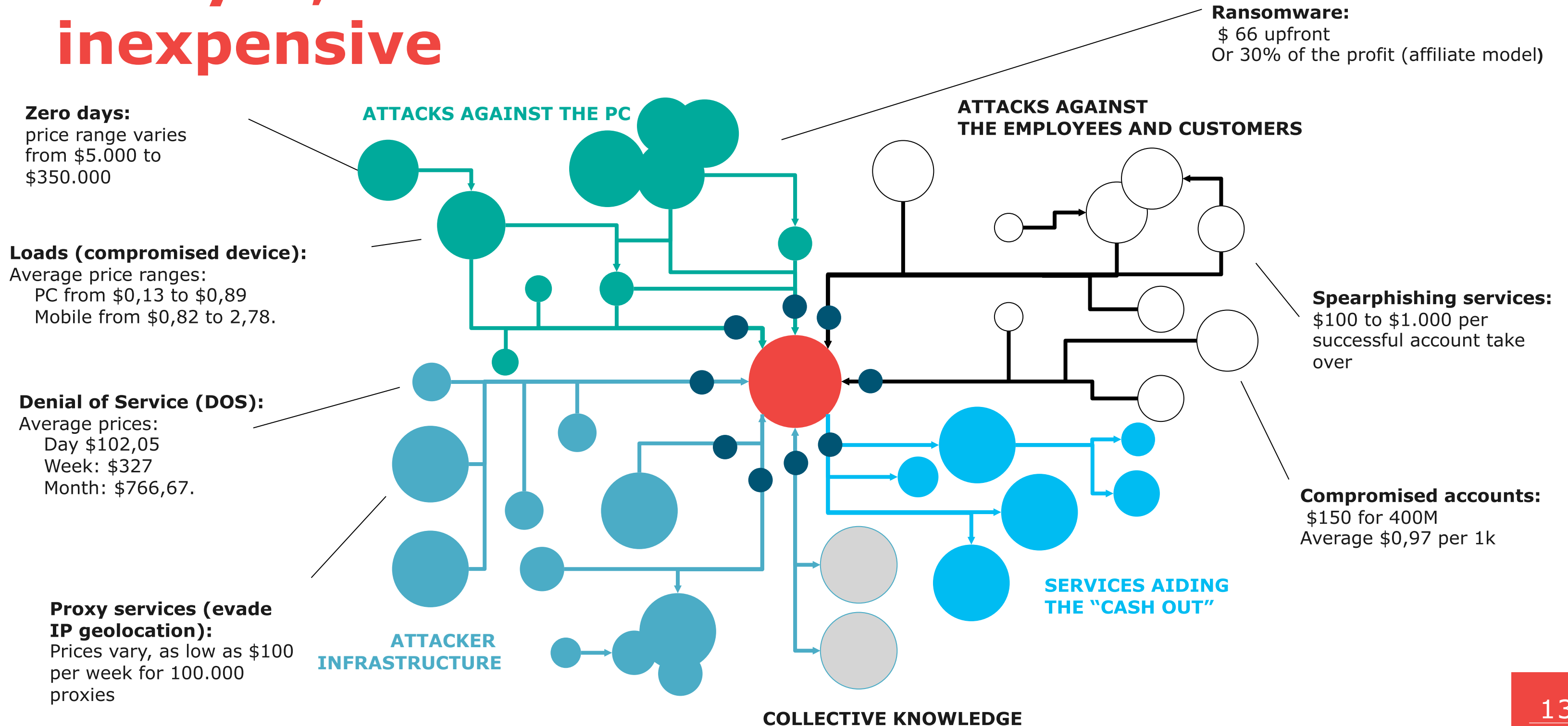
02

Cybercrime trends and defense mechanisms

Most attackers have a supply chain

You face **ecosystems**, not just hackers and malware

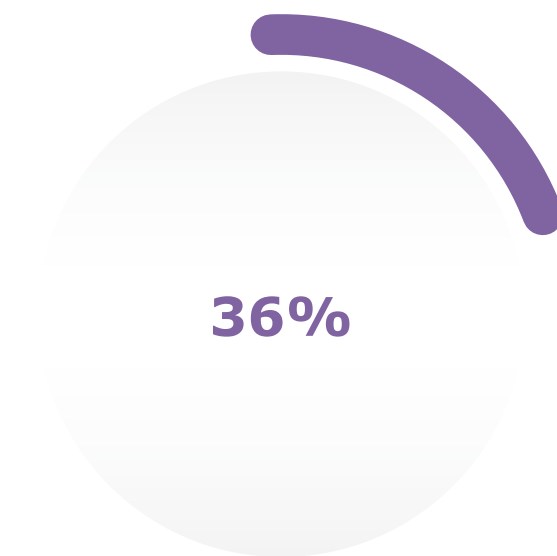Defenses must address *current* attacker methods

ATTACKS AGAINST PCs

ATTACKS AGAINST EMPLOYEES AND CUSTOMERS

ATTACKERS

SERVICES AIDING THE "CASH OUT"

ATTACKER INFRASTRUCTURE

COLLECTIVE KNOWLEDGE

And yes, attack services are inexpensive

Ransomware:
 $ 66 upfront
Or 30% of the profit (affiliate model)

ATTACKS AGAINST THE PC

ATTACKS AGAINST THE EMPLOYEES AND CUSTOMERS

Zero days:
price range varies from $5.000 to $350.000

Loads (compromised device):
Average price ranges:
    PC from $0,13 to $0,89
    Mobile from $0,82 to 2,78.

Spearphishing services:
$100 to $1.000 per successful account take over

Denial of Service (DOS):
Average prices:
    Day $102,05
    Week: $327
    Month: $766,67.

Compromised accounts:
 $150 for 400M
Average $0,97 per 1k

SERVICES AIDING THE "CASH OUT"

Proxy services (evade IP geolocation):
Prices vary, as low as $100 per week for 100.000 proxies

ATTACKER INFRASTRUCTURE

COLLECTIVE KNOWLEDGE

13

Ransomware remains #1 Threat for most organizations, especially healthcare

36%

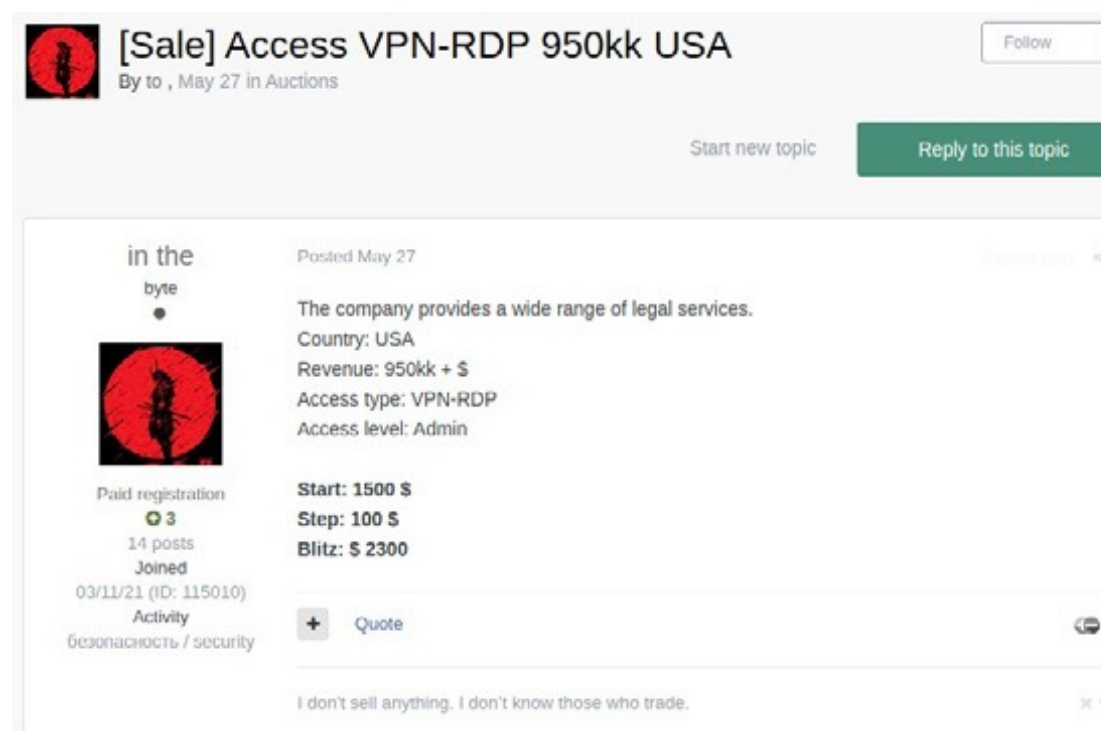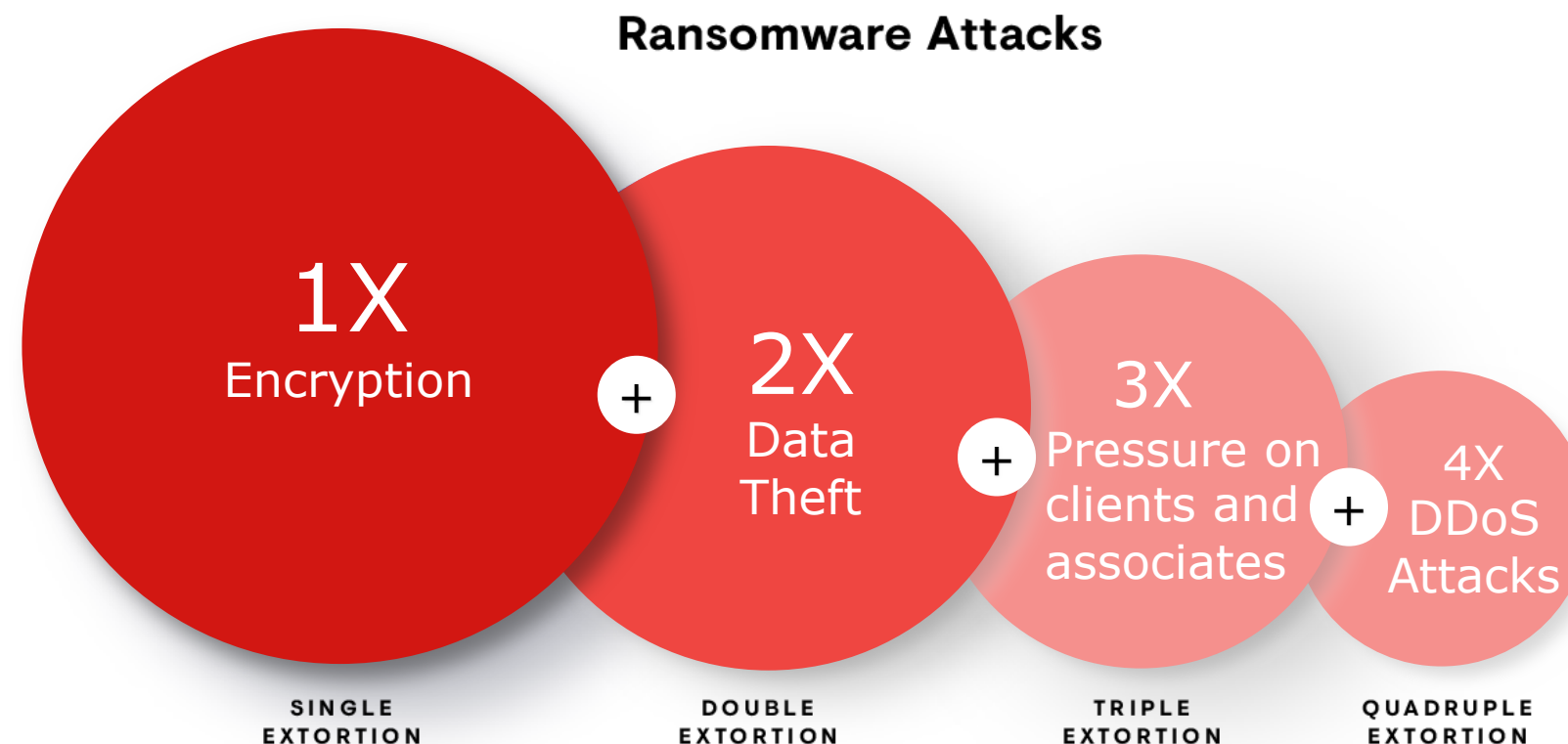**Increase of ransomware attacks in 2020** across the industry

59%

Of the healthcare organizations where suffering from **ransomware attacks**

14

Source: https://www.safetydetectives.com

Ransomware "more impact than before"

- Ransomware-as-a-service
- Multiple monetization tracks
- Name-and-shame
- Ultimately, ransomware attacks occur where access can be most easily obtained and maintained.
- Access for sale – IAB (initial Access Broker)

Ransomware Attacks

1X Encryption
+
2X Data Theft
+
3X Pressure on clients and associates
+
4X DDoS Attacks

SINGLE EXTORTION | DOUBLE EXTORTION | TRIPLE EXTORTION | QUADRUPLE EXTORTION

[Sale] Access VPN-RDP 950kk USA
By to , May 27 in Auctions

Follow 1

Start new topic | Reply to this topic

in the byte

Posted May 27

The company provides a wide range of legal services.
Country: USA
Revenue: 950kk + $
Access type: VPN-RDP
Access level: Admin

Paid registration
3
14 posts
Joined
03/11/21 (ID: 115010)
Activity
безопасность / security

Start: 1500 $
Step: 100 $
Blitz: $ 2300

Quote

I don't sell anything. I don't know those who trade.
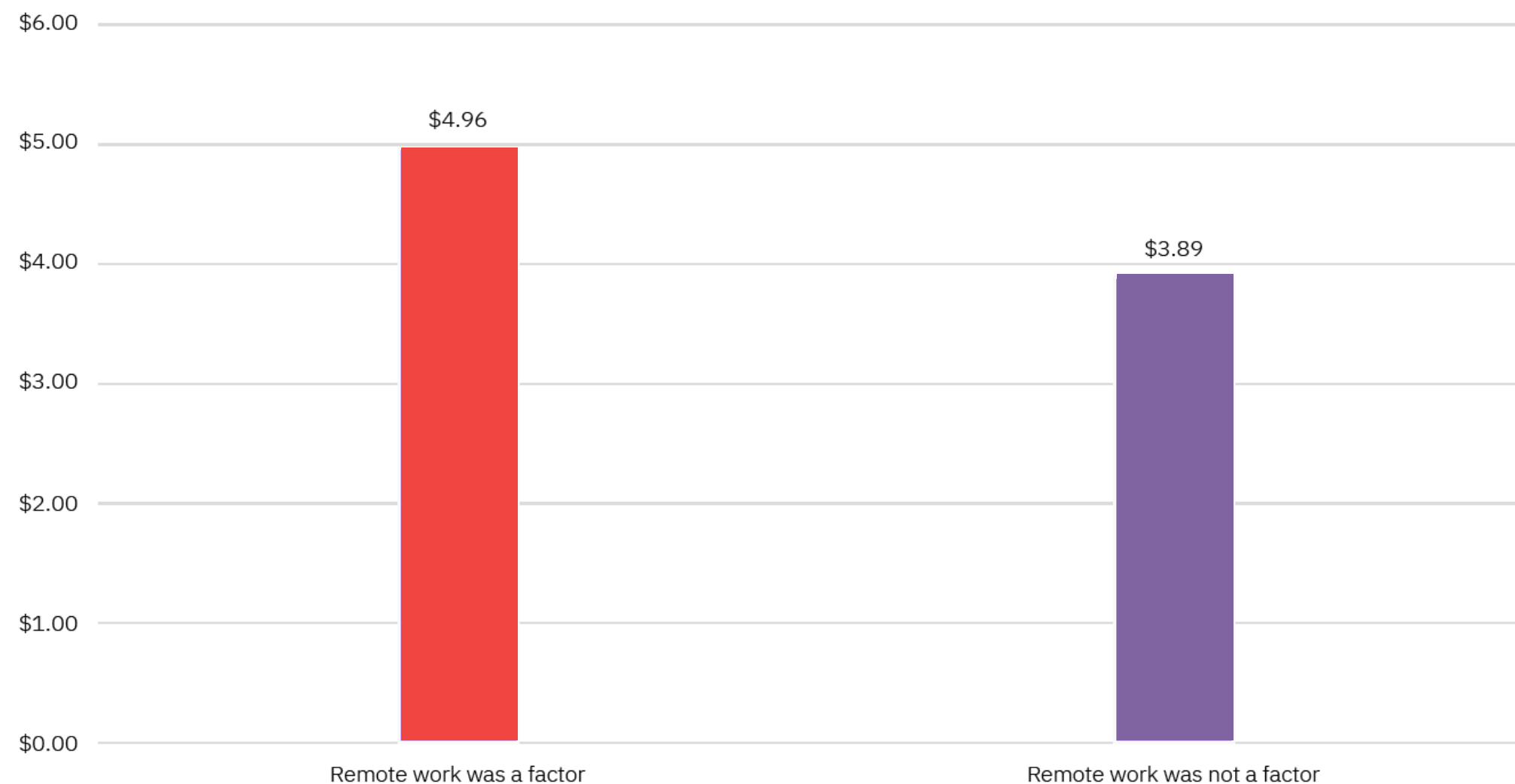
Protect against Ransomware

- Organizations can protect themselves
  - Patch regularly and promptly
  - Protect external facing applications with MFA
  - Principle of least privilege
  - Segment networks
  - Implement endpoint and network traffic monitoring and detection

Patching

\+

Monitoring & Detection

\+

Principle of least privilege

\+

Multi-Factor authentication

=

Protection against ransomware attacks
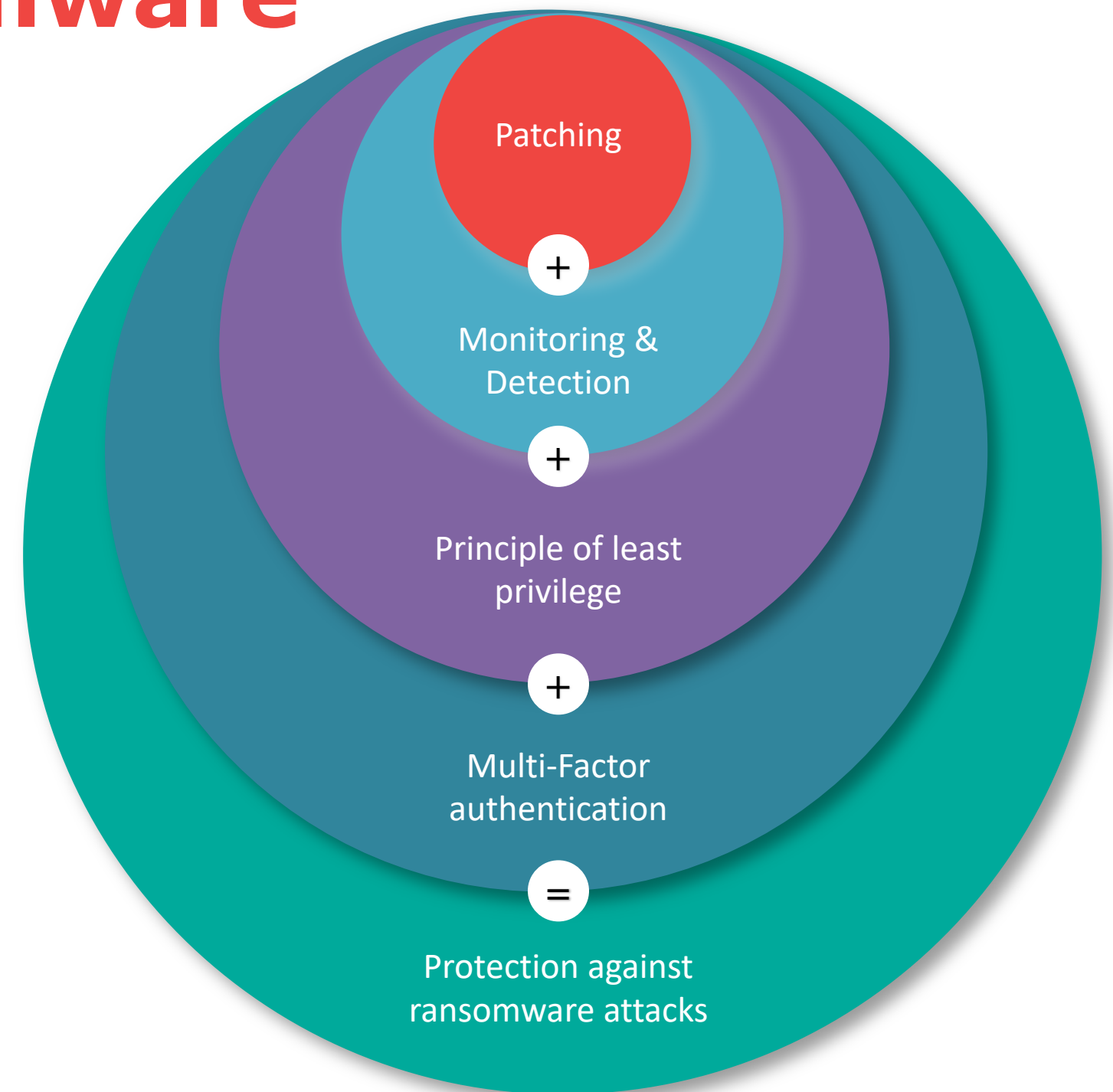
The COVID-19 affect and impact on cost

inetum.
realdolmen
Positive digital flow

$ 1.07m

Cost difference where remote work was a factor in causing the breach

Remote working and digital transformation due to the COVID-19 pandemic increased the average total cost of a data breach

Average cost of a data breach where remote work was a factor

Measured in US$ millions

Bar chart showing: Remote work was a factor $4.96; Remote work was not a factor $3.89. Y-axis from $0.00 to $6.00.
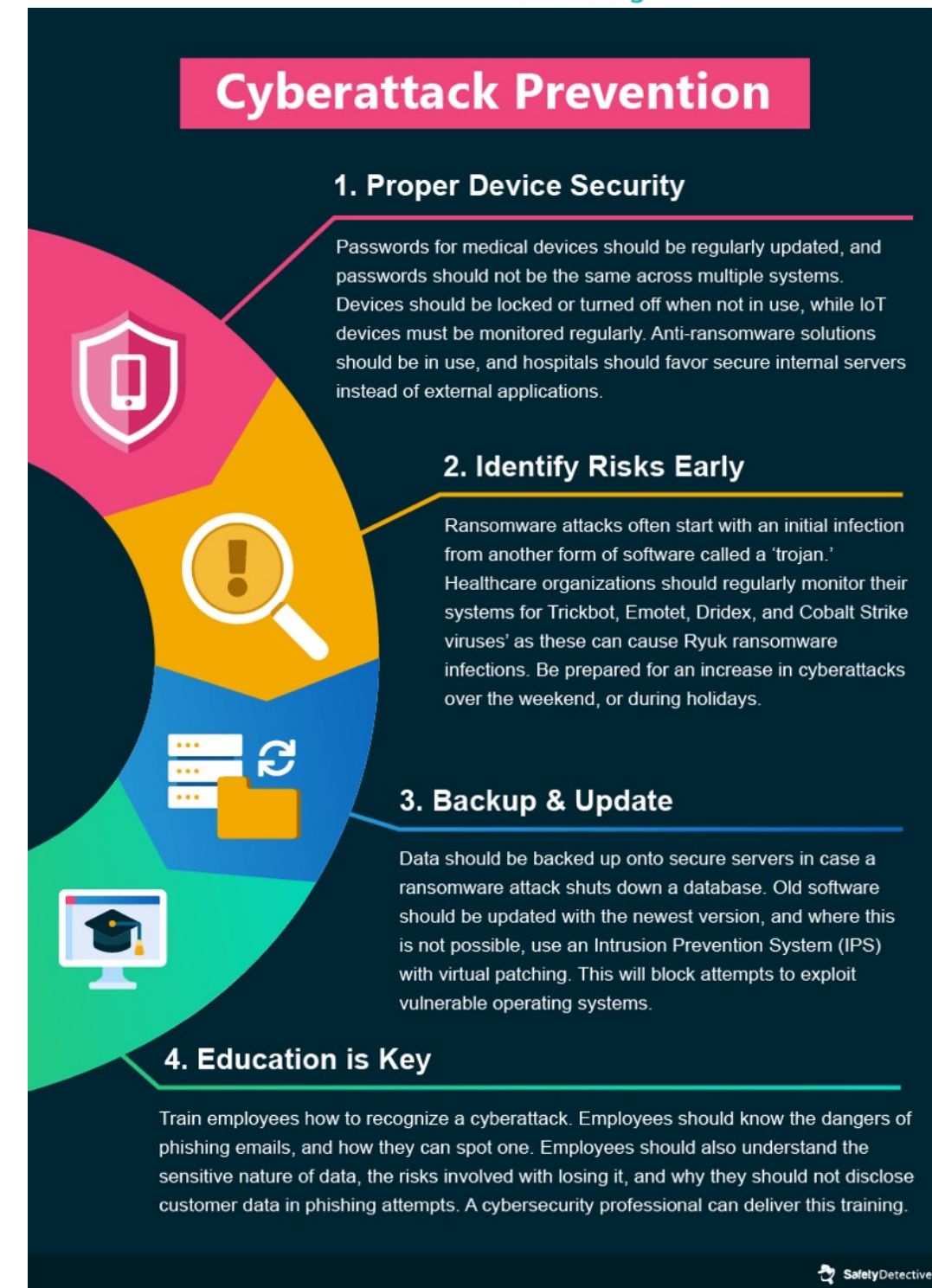
Source:
IBM Breach Report

17

The COVID-19 effect

- Healthcare resources stretched, vigilance diminished

- Critical nature of data makes healthcare attractive target

- COVID-19 rising Healthcare Cybercrime scams
  - COVID-19 Phishing
  - Big Health Data Breaches
  - Tracked logins
  - COVID-19 apps (85% of COVID-19 tracking apps leak data)
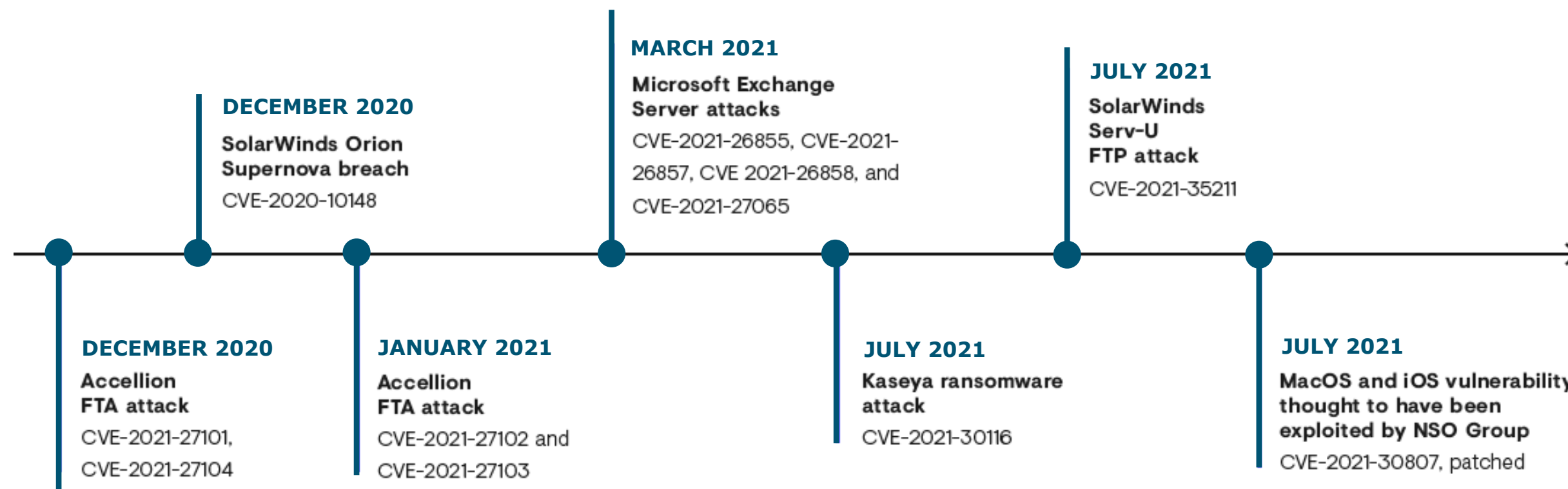 - Working from home (less social control)

The COVID-19 effect:
High profile Data Leaks

- Pfizer Breach
  - On Dec 9th 2020 EMA announced that hackers had stolen data on the vaccine candidate

- Wales Patient Data Breach
  - COVID-19 patient data for 18,000 Welsh residents was leaked due to employee mistake

- Brazil COVID-19 Data Breach
  - Personal details and health information of 16 million Brazilian citizens was exposed due to employee error

- Germany COVID-19 Tracking App
  - Remote Code Execution (RCE) vulnerability in the construction of the Corona-Warn-App.

inetum.
realdolmen
Positive digital flow

Cyberattack Prevention

1. Proper Device Security

Passwords for medical devices should be regularly updated, and passwords should not be the same across multiple systems. Devices should be locked or turned off when not in use, while IoT devices must be monitored regularly. Anti-ransomware solutions should be in use, and hospitals should favor secure internal servers instead of external applications.

2. Identify Risks Early

Ransomware attacks often start with an initial infection from another form of software called a 'trojan.' Healthcare organizations should regularly monitor their systems for Trickbot, Emotet, Dridex, and Cobalt Strike viruses' as these can cause Ryuk ransomware infections. Be prepared for an increase in cyberattacks over the weekend, or during holidays.

3. Backup & Update

Data should be backed up onto secure servers in case a ransomware attack shuts down a database. Old software should be updated with the newest version, and where this is not possible, use an Intrusion Prevention System (IPS) with virtual patching. This will block attempts to exploit vulnerable operating systems.

4. Education is Key

Train employees how to recognize a cyberattack. Employees should know the dangers of phishing emails, and how they can spot one. Employees should also understand the sensitive nature of data, the risks involved with losing it, and why they should not disclose customer data in phishing attempts. A cybersecurity professional can deliver this training.

SafetyDetectives

Increase in Zero day risks, please patch

- **Patch or be punished**
- Scan-and-exploit
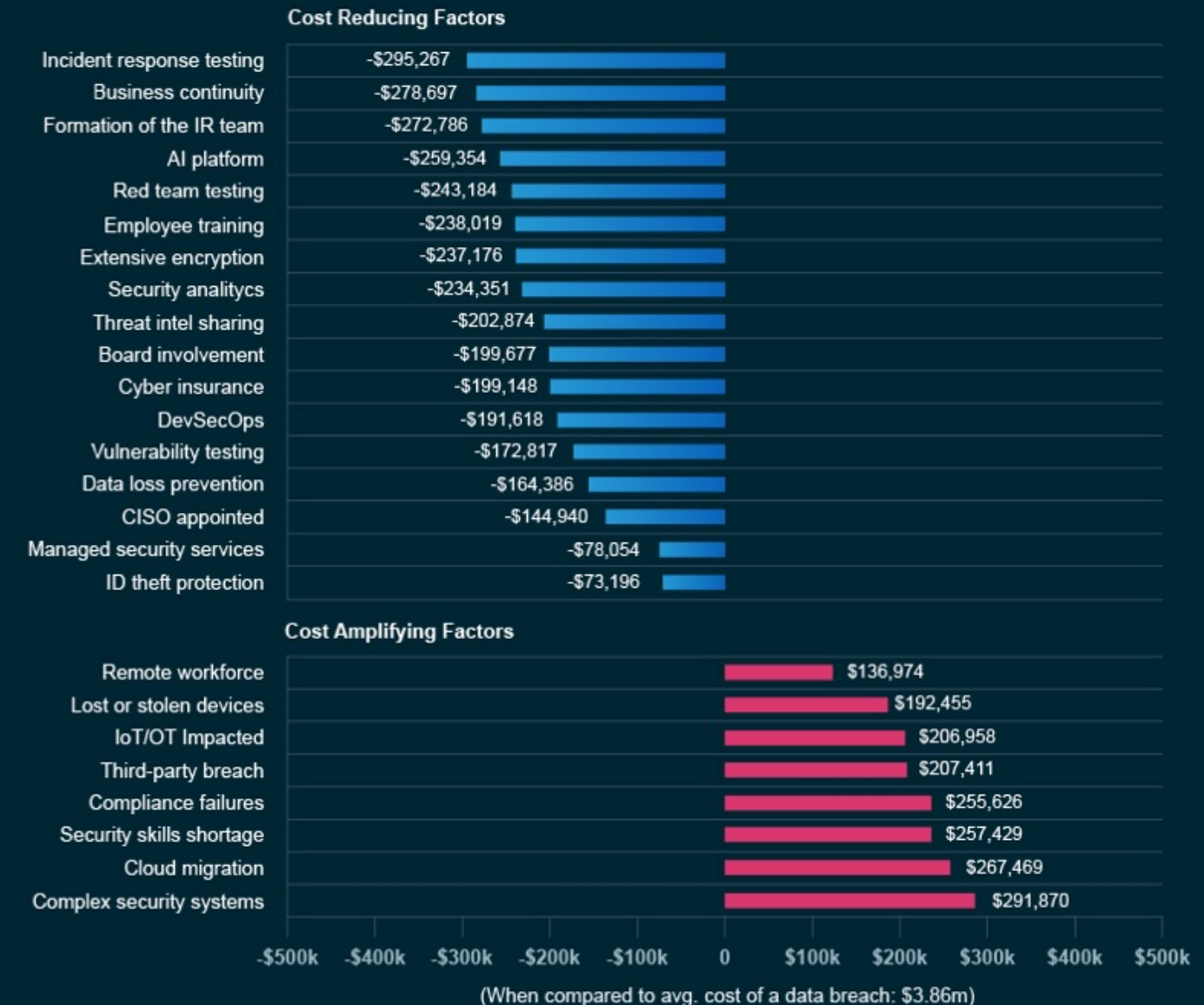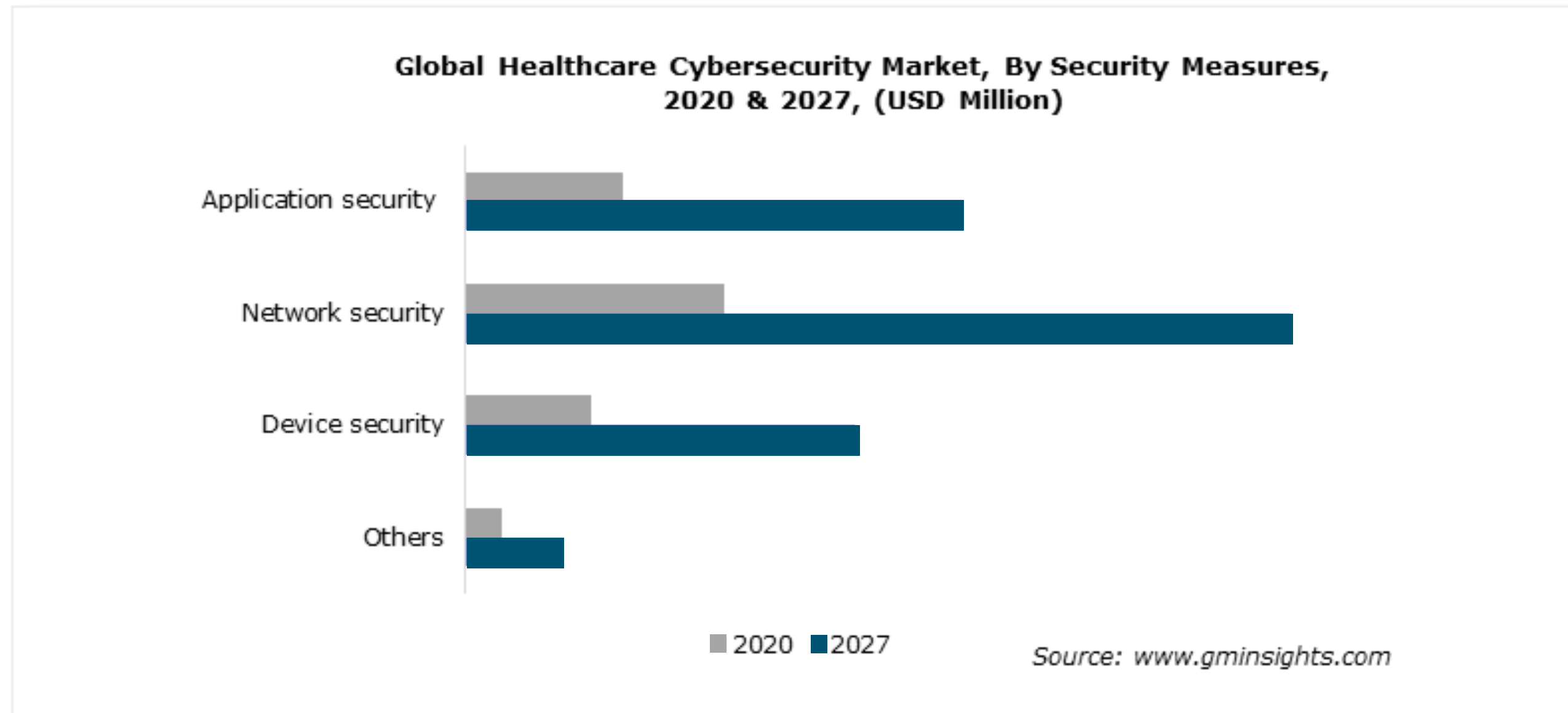- Implement good vulnerability management & layered security controls

DECEMBER 2020

SolarWinds Orion
Supernova breach

CVE-2020-10148

MARCH 2021

Microsoft Exchange
Server attacks

CVE-2021-26855, CVE-2021-
26857, CVE 2021-26858, and
CVE-2021-27065

JULY 2021

SolarWinds
Serv-U
FTP attack

CVE-2021-35211

DECEMBER 2020

Accellion
FTA attack

CVE-2021-27101,
CVE-2021-27104

JANUARY 2021

Accellion
FTA attack

CVE-2021-27102 and
CVE-2021-27103

JULY 2021

Kaseya ransomware
attack

CVE-2021-30116

JULY 2021

MacOS and iOS vulnerability
thought to have been
exploited by NSO Group

CVE-2021-30807, patched

Risk of IoT in healthcare

- IoT provides valuable medical data to help treatment and diagnosis

- **60%** of healthcare providers incorporate IoT into facilities

- IoT devices vulnerable

- Study shows that internet-connected medical imaging machines (eg MRI) are susceptible to attacks. **In 2020, 83% of devices were vulnerable to hackers an increase of 56% compared with 2018**

- DDoS attack could cripple patient care

Many Factors Impact The Cost of a Data Breach

Some of these factors can have a positive impact, others can have a negative impact. Organizations need to ensure they have adequate systems in place to reduce the cost of a data breach by addressing each factor.

Cost Reducing Factors

Factor	Cost
Incident response testing	-$295,267
Business continuity	-$278,697
Formation of the IR team	-$272,786
AI platform	-$259,354
Red team testing	-$243,184
Employee training	-$238,019
Extensive encryption	-$237,176
Security analitycs	-$234,351
Threat intel sharing	-$202,874
Board involvement	-$199,677
Cyber insurance	-$199,148
DevSecOps	-$191,618
Vulnerability testing	-$172,817
Data loss prevention	-$164,386
CISO appointed	-$144,940
Managed security services	-$78,054
ID theft protection	-$73,196

Cost Amplifying Factors

Factor	Cost
Remote workforce	$136,974
Lost or stolen devices	$192,455
IoT/OT Impacted	$206,958
Third-party breach	$207,411
Compliance failures	$255,626
Security skills shortage	$257,429
Cloud migration	$267,469
Complex security systems	$291,870

(When compared to avg. cost of a data breach: $3.86m)

SafetyDetectives

Forecast about security focus of healthcare industry 2020 -2027

Global Healthcare Cybersecurity Market, By Security Measures, 2020 & 2027, (USD Million)

Source: www.gminsights.com

Source: https://www.gminsights.com

Impact of security incidents

Figure 2: Significant Security Incidents – Impact of Incident

NO IMPACT OR NEGLIGIBLE IMPACT	34%
DISRUPTION OF SYSTEMS/DEVICES IMPACTING IT OPERATIONS	28%
DISRUPTION OF SYSTEMS/DEVICES IMPACTING BUSINESS OPERATIONS	27%
DATA BREACH OR DATA LEAKAGE	21%
MONETARY LOSS	20%
DISRUPTION OF SYSTEMS/DEVICES IMPACTING CLINICAL CARE	15%
DAMAGE OR DESTRUCTION OF SYSTEMS/DEVICES IMPACTING BUSINESS OPERATIONS	8%
DAMAGE OR DESTRUCTION OF SYSTEMS/DEVICES IMPACTING IT OPERATIONS	5%
DAMAGE OR DESTRUCTION OF SYSTEMS/DEVICES IMPACTING CLINICAL CARE	3%

Figure 3: Significant Security Incidents – Types of Patient Safety Issues

DISRUPTION OF NON-EMERGENCY CLINICAL CARE	61%
DISRUPTION OF EMERGENCY SERVICES	28%
SERIOUS PATIENT INJURY OR HARM	17%
DIVERSION OF PATIENTS TO OTHER FACILITIES	17%
CANCELLATION OF ELECTIVE SURGERIES	17%
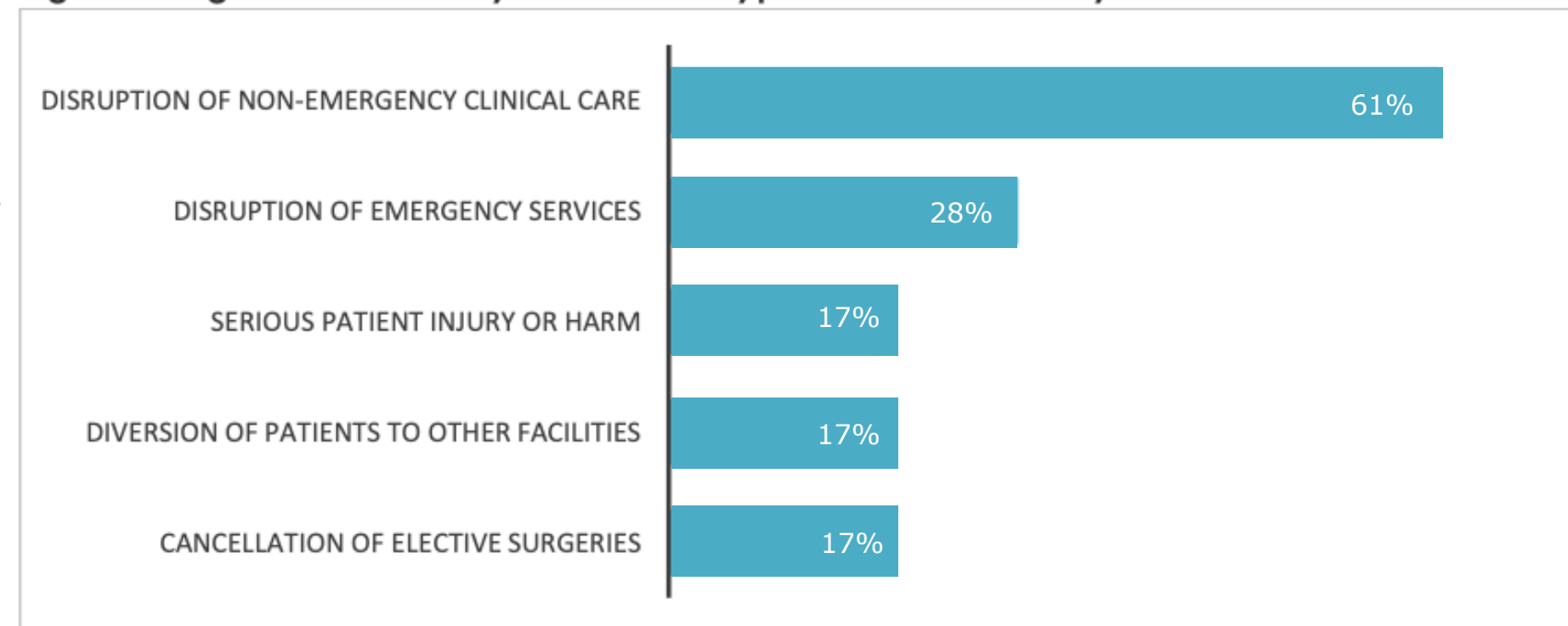
03

Conclusion & key takeaways

"from a risk perspective"

Understand business impact & likelihood of security risks

is your business aware?

Healthcare is N°1

Healthcare is the N°1 target for hackers

Healthcare suffers the highest data breach cost of all industries

Likelihood

59% where suffering from ransomware attacks

83% internet-connected medical imaging machines (eg MRI) are susceptible to attacks. In 2020, 83% of devices were vulnerable to hackers

93% healthcare organizations experienced a data breach the past 3 years of which 30% were hospitals
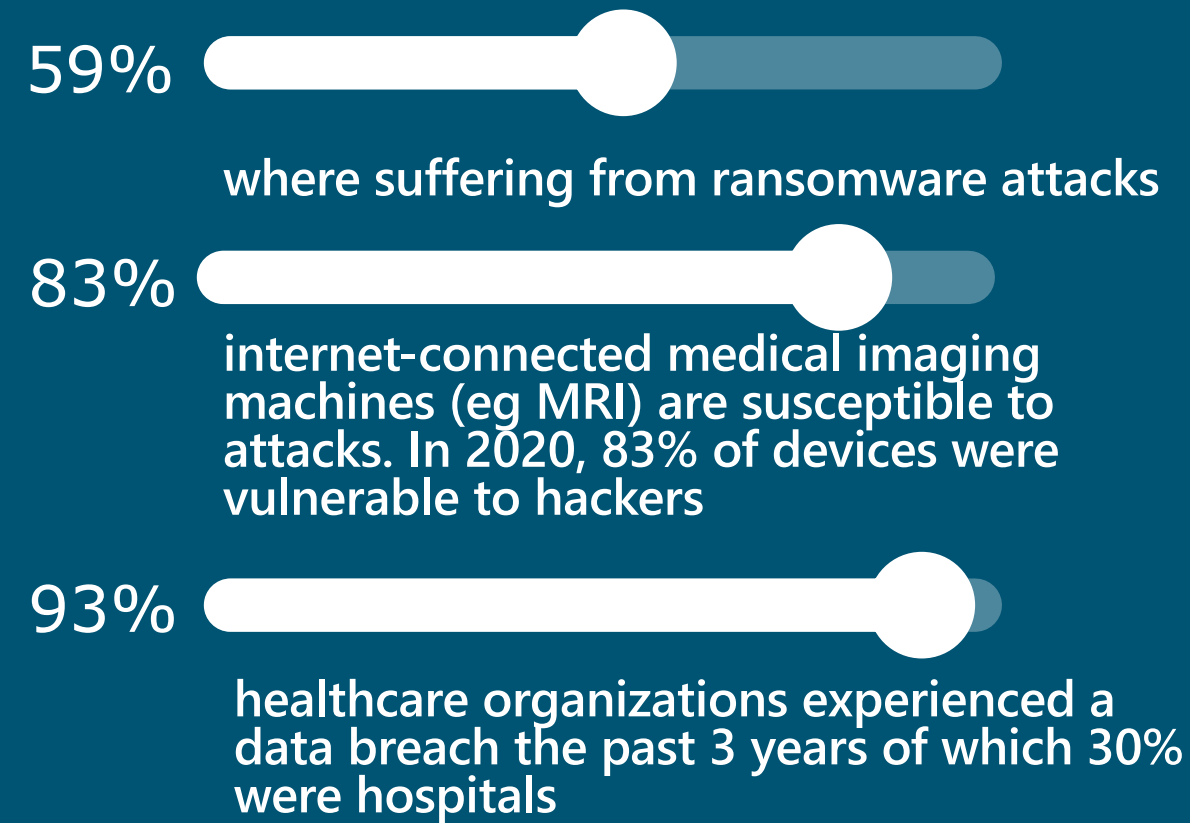
Impact

Healthcare service disruption

> 200 days to Identify and contain an databreach incident.[2]

Brand damage

Financial loss $9.23 million Average cost of databreach.

Patient safety & personal loss (average $2.500)

Key Takeaways

Ransomware remains #1 Threat for most organizations

Healthcare #1 target for cybercriminals # 1 most expensive data breach costs

Forecast Healthcare industry defense focus next 5 years:
- Device security
- Network security
- Application security

Risk of IoT in healthcare is very high

inetum
realdolmen
Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE