Aligning Privacy & Security Investments to Business Value

นพ. ประดิษฐ์ สมประกิจ

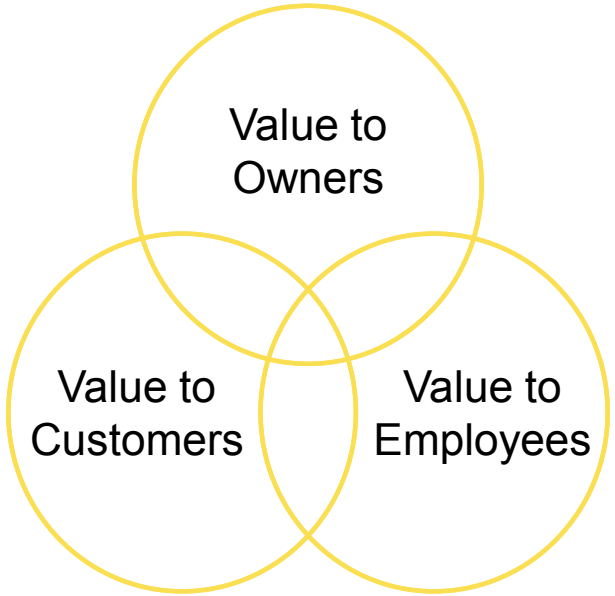
28 พฤษภาคม 2568

BDMS Bangkok Dusit Medical Services GREENLINE SYNERGY BNH HOSPITAL SINCE 1898

What is “Business Value”? Whose viewpoint?

- *Value is defined as outcomes relative to costs and value should always be define around the customer*
- *In any field, improving performance and accountability depends on having a shared goal that unites the interests and activities of all stakeholders.*

Micheal E. Porter. What is value in Health Care?
The New England Journal of Medicine. December 23, 2010.

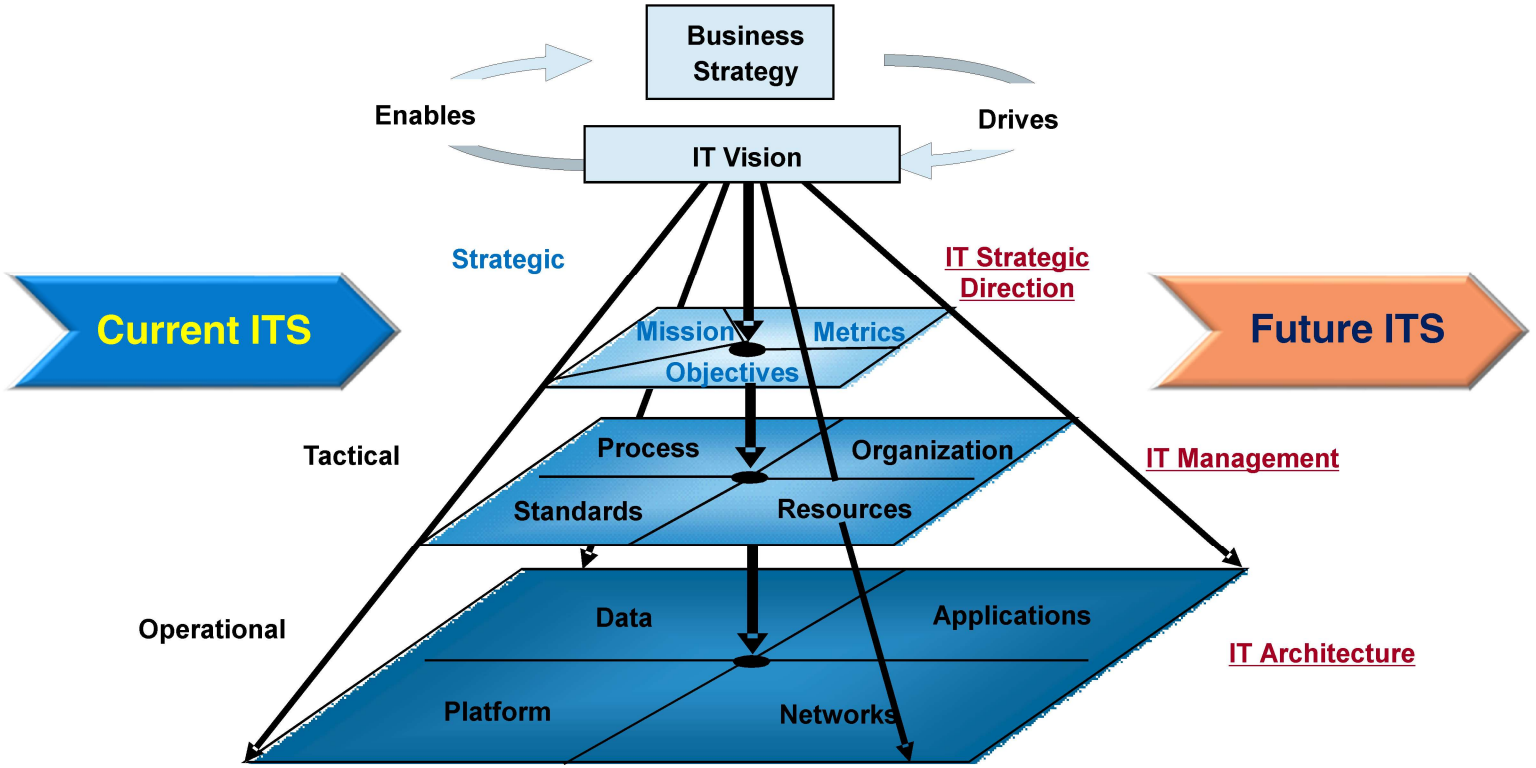


Alignment of IT Strategy with Business Strategy is Key…

Internal / External
Strength / Opportunity
Weakness / Threat
Competitors

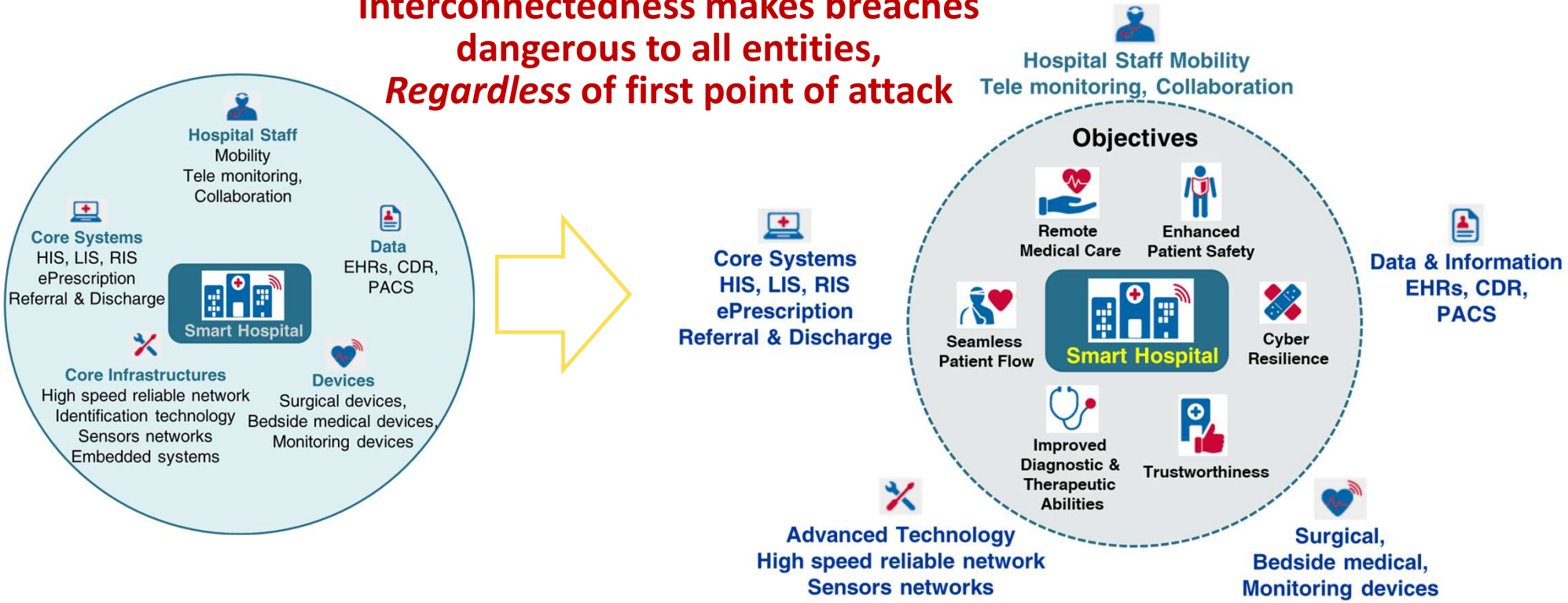
IT Governance
Organization Strategy & IT Strategies
Current relevance in today's environment…

Measurement / Monitoring



What is a "Smart" Hospital?

Interconnectedness makes breaches dangerous to all entities, *Regardless* of first point of attack



*"A smart hospital is a hospital that relies on **optimised** and **automated processes** built on an **ICT** environment of **interconnected assets**, particularly based on **Internet of things (IoT)**, to **improve existing patient care procedures** and **introduce new capabilities**"*

Modified from: www.enisa.europa.eu. Smart Hospital, Nov 2016.

Security & Privacy

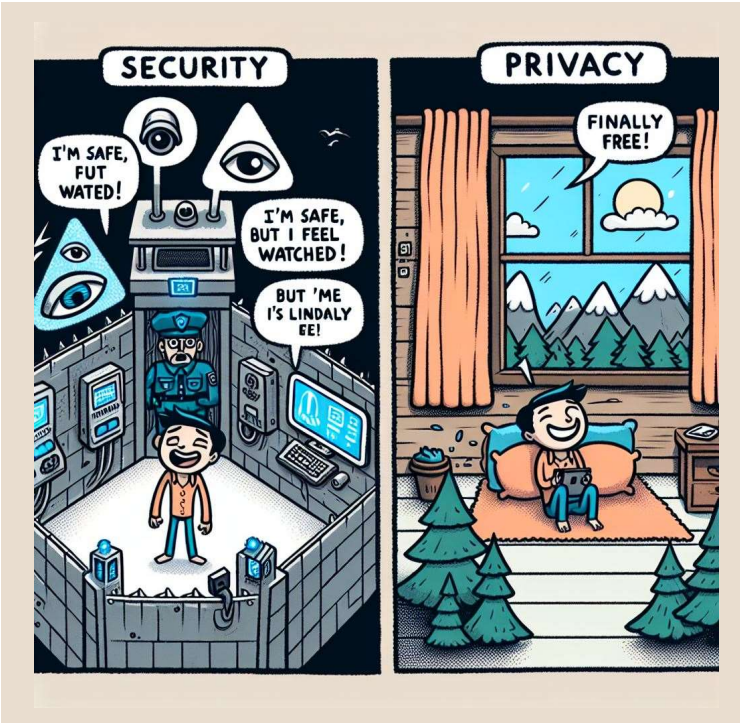
ความมั่นคงปลอดภัย

Confidentiality

Integrity

Availability

“Security is crucial for safeguarding privacy and often concentrates on the technical aspects, such as encryption, firewalls, and disaster recovery”



ความเป็นส่วนตัว

- ✓ เท่ากับความลับ (Confidentiality)?
- ✓ วัฒนธรรม, มารยาท, กฎหมาย
- ✓ ความเป็นส่วนตัว - สิทธิ์ที่จะกำหนดให้ “ใครเก็บข้อมูลอะไรของเรา? เพื่ออะไร? เปิดเผยให้ใครได้บ้าง?
- ✓ เรื่องส่วนตัวที่เราบอกให้คนทราบบ่อย ๆ ยังถือเป็นเรื่องส่วนตัวหรือไม่?
- ✓ เรื่องส่วนตัวที่เราไม่ค่อยบอกให้ผู้อื่นรับรู้ หรือไม่บอกเลย = ความลับ?

พระราชบัญญัติสุขภาพแห่งชาติ ๒๕๕๐

มาตรา ๗ ข้อมูลด้านสุขภาพของบุคคล เป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรง หรือ มีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใด ๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้

พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- ✓ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง
- ✓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๕๗ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท
- ✓ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. หรือขัดขวางหรือไม่ปฏิบัติตามตามคำสั่งของ กกม. ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรงโดยไม่มีเหตุอันสมควร มีโทษจำ หรือปรับ หรือทั้งจำและปรับ

กกม. = คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) ด้านความมั่นคงของรัฐ

(๒) ด้านบริการภาครัฐที่สำคัญ

(๓) ด้านการเงินการธนาคาร

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(๕) ด้านการขนส่งและโลจิสติกส์

(๖) ด้านพลังงานและสาธารณูปโภค

(๗) ด้านสาธารณสุข

(๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

การพิจารณาประกาศกำหนดภารกิจหรือบริการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ คณะกรรมการจะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม

พรบ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

(๑) จัดให้มีและทบทวนมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ข้อ ๓ ในประกาศนี้

"ความมั่นคงปลอดภัย" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ

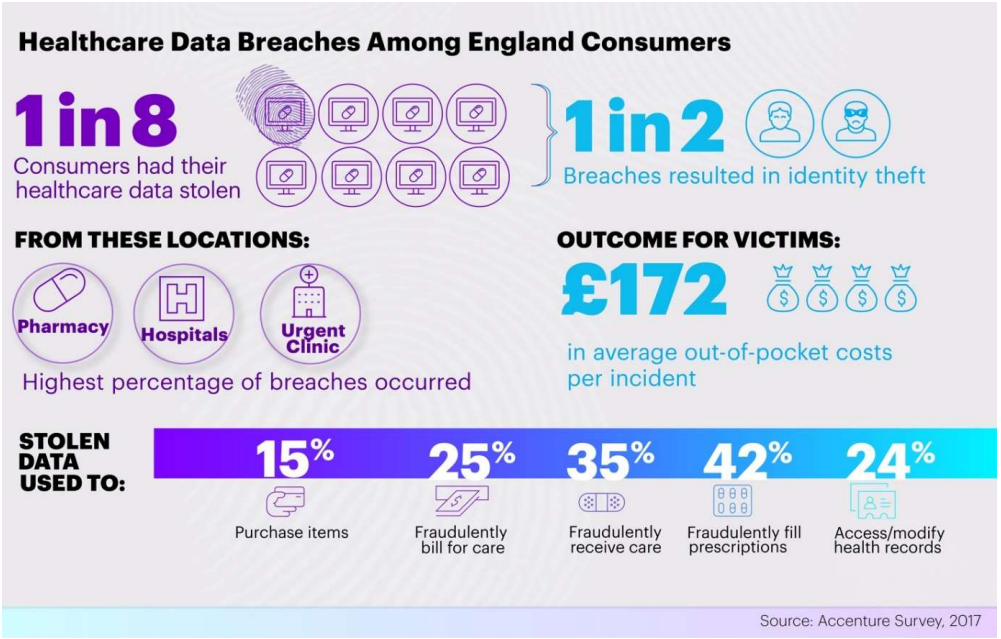
Major Cyber attack on NHS England: WannaCry attack

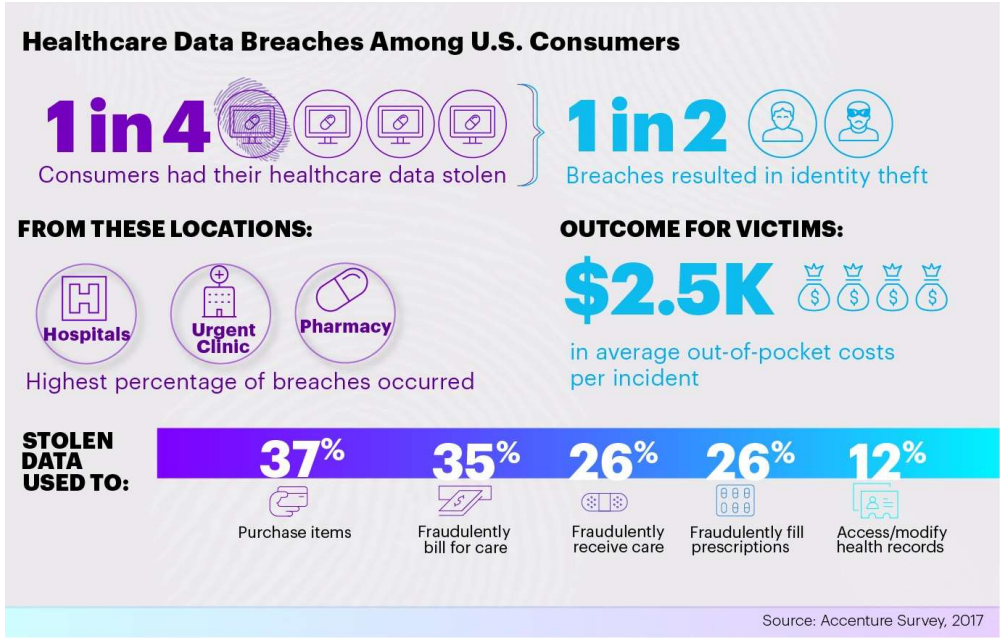
What happened

- A cyber-attack that affected more than 60 trusts within the United Kingdom's National Health Service (NHS) has spread to more than 200 000 computer systems in 150 countries, including Canada. ….
- On May 12, the "WannaCry" ransomware began affecting dozens of NHS facilities. Eventually, more than 60 NHS trusts were hit. Many facilities could not access patient records, which led to delays of non-urgent surgeries and cancelled patient appointments. Some hospitals had to divert ambulances to other facilities.
- Although the NHS does not appear to have been specifically targeted by whoever is behind the WannaCry ransomware, it was vulnerable to attack because some of its Windows operating systems are more than 15 years old and were no longer updated or supported by Microsoft.

Collier R. NHS ransomware attack spreads worldwide. CMAJ. 2017 Jun 5; 189 (22): E786–E787.

Personal Data Breach: Sensitive information & Identity Theft





- **Personal health information – Sensitive information**
- **Identity theft – Valuable information**

ZDNet | VIDEOS | EXECUTIVE GUIDES | SECURITY | CLOUD | INNOVATION | CXO | HARDWARE | MORE | NEWSLETTERS | ALL WRITERS

MUST READ: How US authorities tracked down the North Korean hacker behind WannaCry

Singapore suffers 'most serious' data breach, affecting 1.5M healthcare patients including Prime Minister

Government describes attack as "deliberate, targeted, well-planned" and assures no medical data has been tempered with, but security vendors warn compromised data may end up for sale on the Dark Web.

By Eileen Yu for By The Way | July 20, 2018 -- 15:55 GMT (23:55 GMT+08:00) | Topic: Security

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

https://www.securityweek.com/massive-singapore-healthcare-breach-possibly-involved-contractor

Subscribe (Free) | CISO Forum 2018 | ICS Cyber Security Conference | Contact Us

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Security Strategy | SCADA / ICS | IoT Security

Home > Cyberwarfare

Massive Singapore Healthcare Breach Possibly Involved Contractor

By Eduard Kovacs on July 30, 2018

Share | G+ | Tweet | แชร์ 25 | RSS

Researchers have come across two Pastebin posts that could shed more light on the data breach that resulted in the health records of 1.5 million Singaporeans getting stolen by hackers.

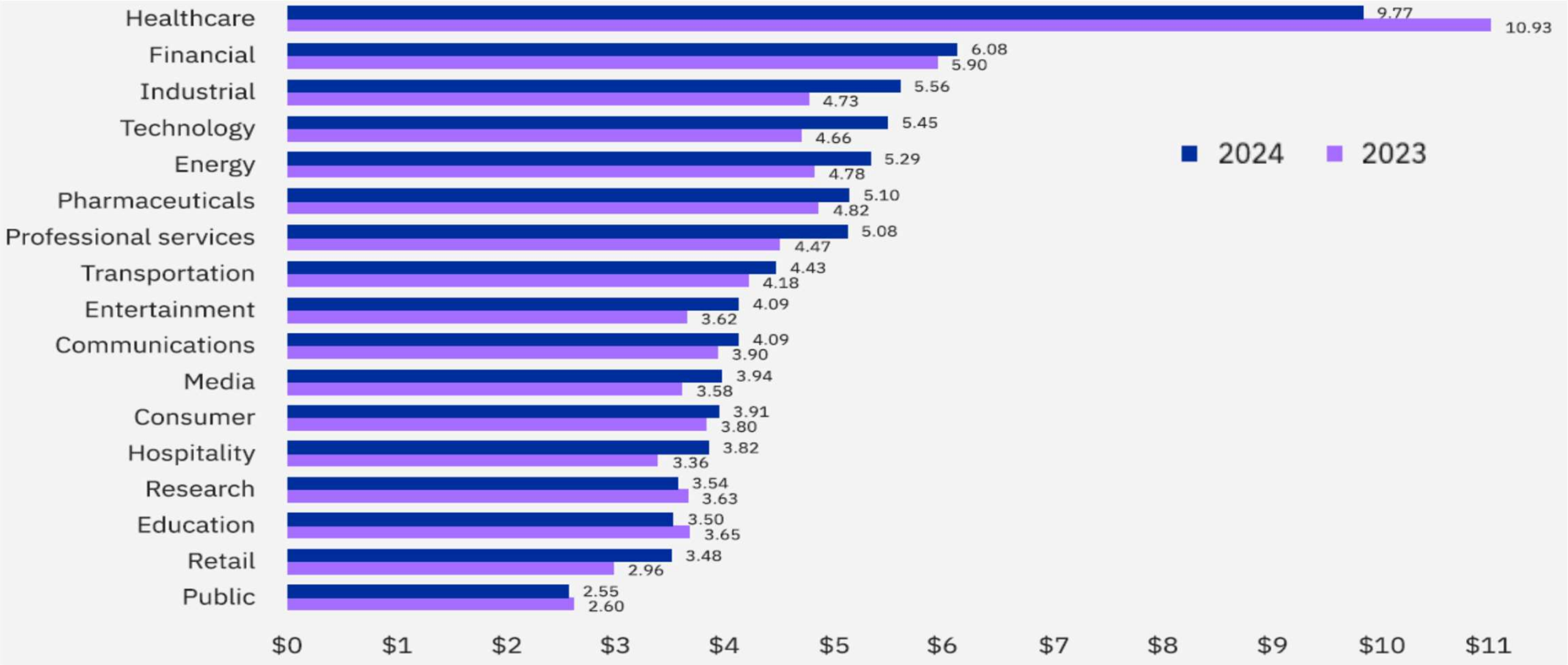
Google™ Custom Search | Search

SECURITYWEEK DAILY BRIEFING

BRIEFING

Business Email Address | SUBSCRIBE

Data Breach Cost by Industry



IBM Cost of a Data Breach Report 2024

Data Breach Cost

USD 4.88M

- The global average cost of a data breach increased 10% over the previous year, reaching USD 4.88 million

USD 2.2M

- Applying security AI and automation is paying off, lowering breach costs in some instances by an average of USD 2.2 million. AI and automation solutions are reducing the lifespan needed to identify and contain a breach and its resulting damage.

46%

- 46% of breaches involving customer personal data. Intellectual property (IP) records came in a close second (43% of breaches).

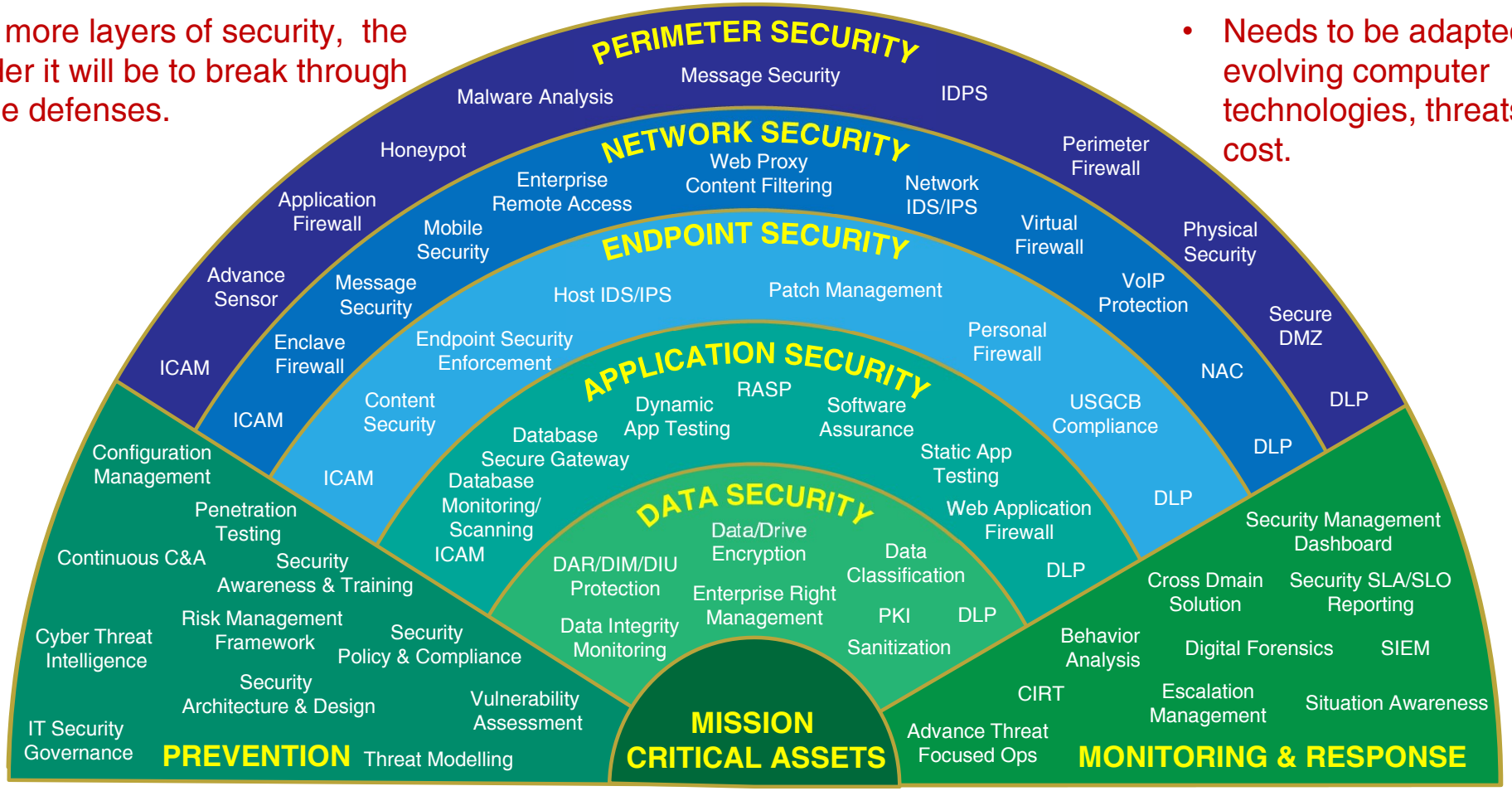
USD 1M

- Cost savings when law enforcement is involved in ransomware attacks by an average of nearly USD 1 million, and also helped shorten the time required to identify and contain breaches from 297 days to 281 days.

IBM Cost of a Data Breach Report 2024

Cyber Security Defense in Depth

- The more layers of security, the harder it will be to break through these defenses.
- Needs to be adapted to evolving computer technologies, threats & cost.

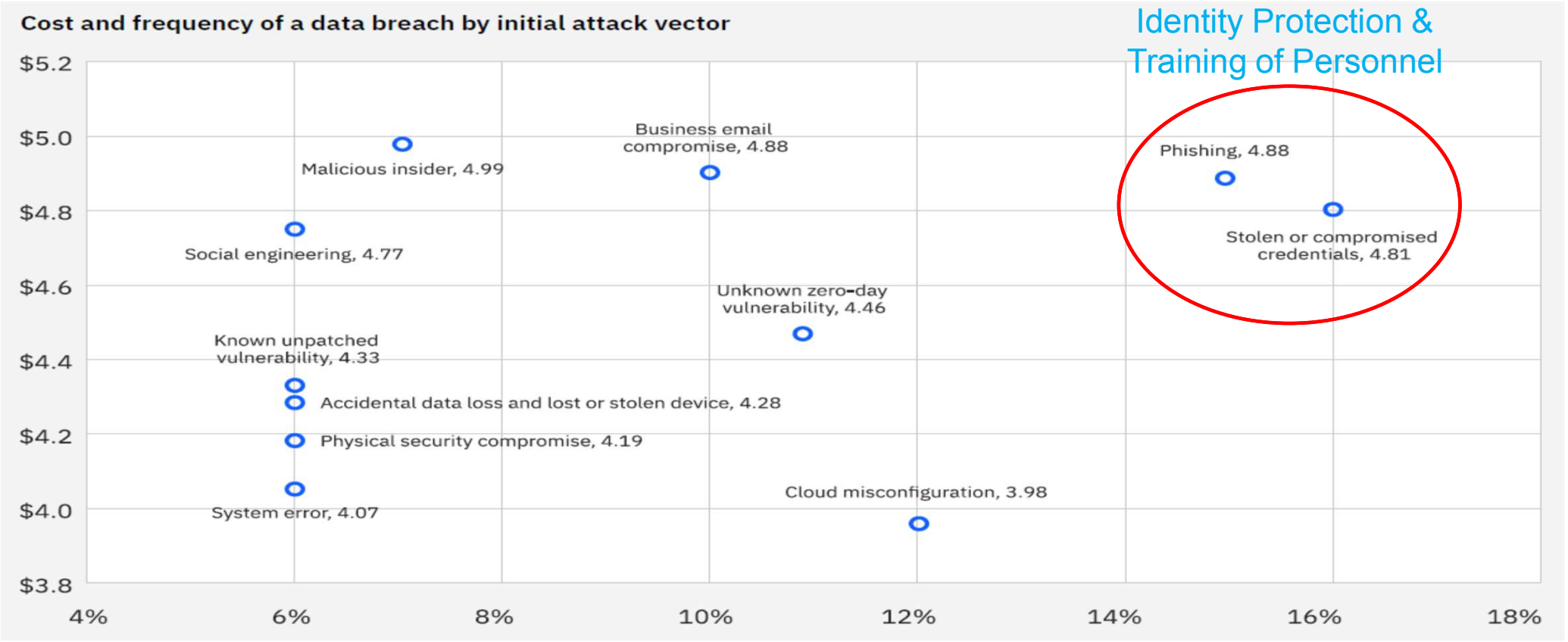


- Information Classification & Handing
- Crisis Management
- Risk Management
- Data Protection & Privacy
- Vulnerability Management Policy
- Service Continuity Management

Security Policies & Standards

- Physical Security
- Secure Cloud Delivery
- Supplier Security
- Business Continuity Management
- Disaster Recovery Management
- Secure Systems Operations

Initial attack vectors and root causes



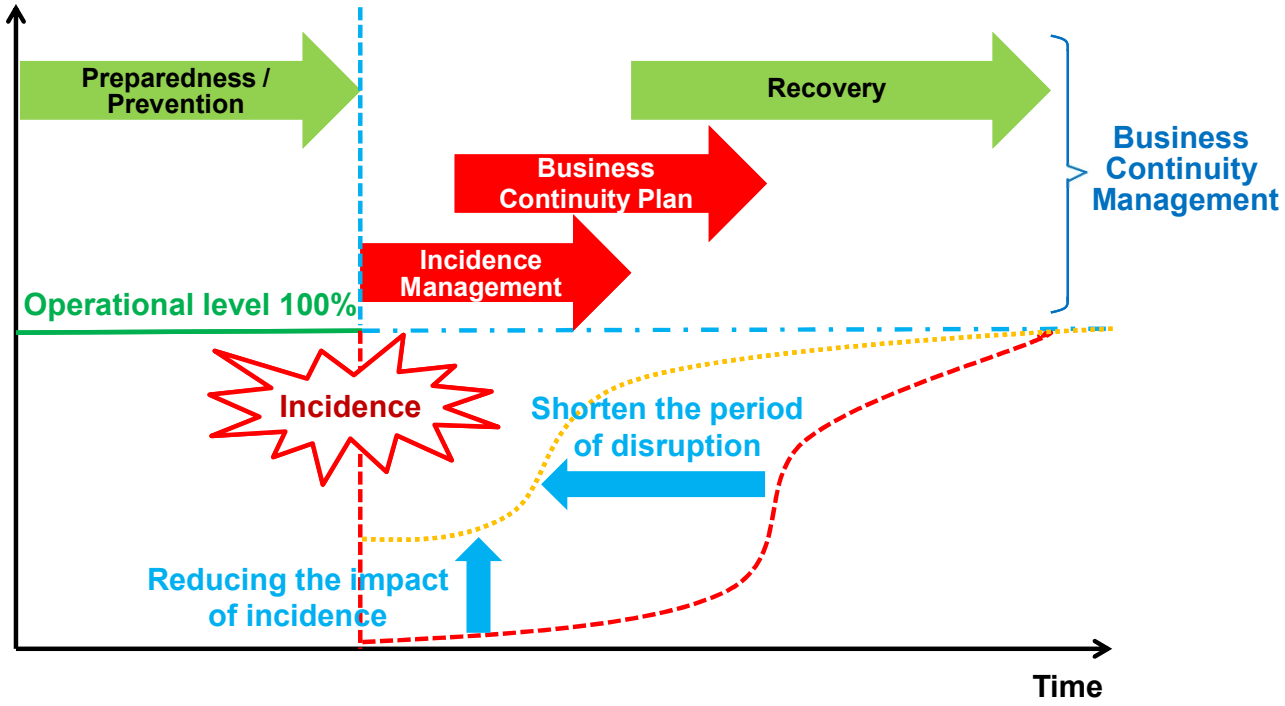
IBM Cost of a Data Breach Report 2024

Key differences between cloud and on-premise security strategies

The choice will depend on the unique requirements of the organization, e.g., its size, budget limitations, security needs, maintenance factors, and adherence to legal standards. If they prioritize scalability and reduced maintenance responsibilities may opt for cloud solutions, whereas those want to fully control over their systems and be able to dedicate internal resources might favor on-premises alternatives.

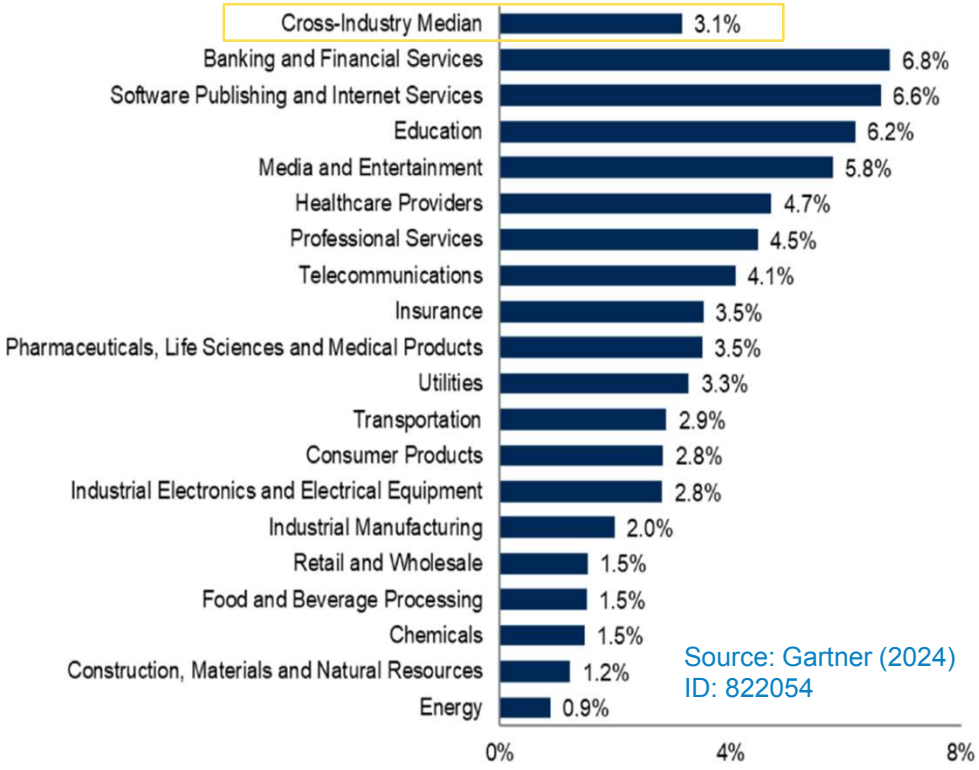
Factor	Public Cloud	On-Premise
1. **Control & Management**	Mainly by cloud providers. Typically built and benchmarked against international security standards certifications, e.g., ISO, HIPAA for health data, PCI for credit cards	Fully managed and responsible by organization.
2. **Scalability**	Highly scalable	Limited scalability
3. **Cost**	Subscription model, ↓ need for large capital expenditure	Requires significant upfront investment & ongoing maintenance costs
4. **Maintenance & Updates**	Handled by the cloud provider – the latest security patches are always in place	Is the responsibility of the organization and can be resource-intensive.
5. **Accessibility**	Anywhere with an internet connection, providing flexibility for remote work & collaboration	Typically restricted to the physical location of the infrastructure, limiting remote access
6. **Compliance & Data Sovereignty**	Can be more complex due to data stored off-site and potentially in different jurisdictions	Easier to ensure compliance with local regulation due to data stored on-site and under direct control
7. **Disaster recovery**	Often includes build-in disaster recovery solution	Requires the organization own DR plan

Back-up plan – Business Continuity Management



% IT Spending/Revenue & %IT Risk Investment

IT Spending as a Percent of Revenue



Source: Gartner (2024)
ID: 822054

- % IT Investments are different among industries.
- This may reflect how IT investment are critical to their value.

Executive Summary
IT Security

Source: Gartner (2024)
ID: 822104

Key Findings

- For 2024, median IT security and risk management investment accounts for 5.6% of total IT spending up from 5.5% last year as mandates for risk reduction were at least as important as revenue generation and cost reduction.
- The percentage of IT Security Spending on traditional reactive functions IT Infrastructure Operational Security (Firewalls/anti-virus) continued to fall relative to more proactive functions such as vulnerability and analytics.
- The 2024 median IT security FTEs as a percent of Total IT FTEs is 5.1% down from 5.4% last year. It's possible that growth in other areas such as digitization have outpaced staffing in security, or this may be just sample related.

END
&
THANK YOU