Cyber resilience approach to deal with emerging threats

October 2022

Puneet Kukreja
EY Ireland (UKI) Cyber Leader

Building a better working world

Our world today

The threat landscape in which we operate

Threat Horizon 2022

Digital and physical worlds collide

- 1.1 Augmented attacks distort reality
- 1.2 Behavioural analytics trigger a consumer backlash
- 1.3 Robo-helpers help themselves to data
- 2.1 Edge computing pushes security to the brink
- 2.2 Extreme weather wreaks havoc on infrastructure
- 2.3 The Internet of Forgotten Things bites back
- 3.1 Deepfakes tell true lies
- 3.2 The digital generation become the scammer's dream
- 3.3 Activists expose digital ethics abuse

Threat Horizon 2023

Security at a tipping point

- 1.1 Artificial intelligence industrialises high-impact attacks
- 1.2 Automated defences backfire
- 1.3 Layered security causes complacency and confusion
- 2.1 Digital doppelgängers undermine identity
- 2.2 Biological data drives a rash of breaches
- 2.3 Gamed algorithms cause commercial confusion
- 3.1 Smart grids succumb to an attack surge
- 3.2 Isolationism creates a security disconnect
- 3.3 Security struggles to adjust to the never normal

Threat Horizon 2024

The disintegration of trust

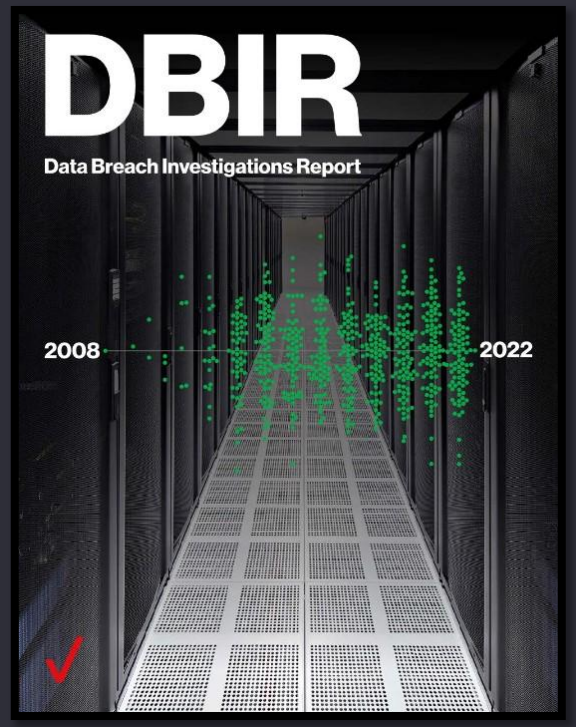
- **1.1 Ransomware evolves into triple extortion**
- **1.2 Regulators inhibit data-driven innovation**
- **1.3 Attackers undermine central cryptocurrencies**
- **2.1 The cloud risk bubble bursts**
- **2.2 Activists pivot to cyber space**
- **2.3 Misplaced confidence disguises low-code risks**
- **3.1 Attackers poison the data well**
- **3.2 Misleading signals subvert cyber fusion centres**
- **3.3 Digital twins double the attack surface**

SOURCE: ISF Threat Horizon Report

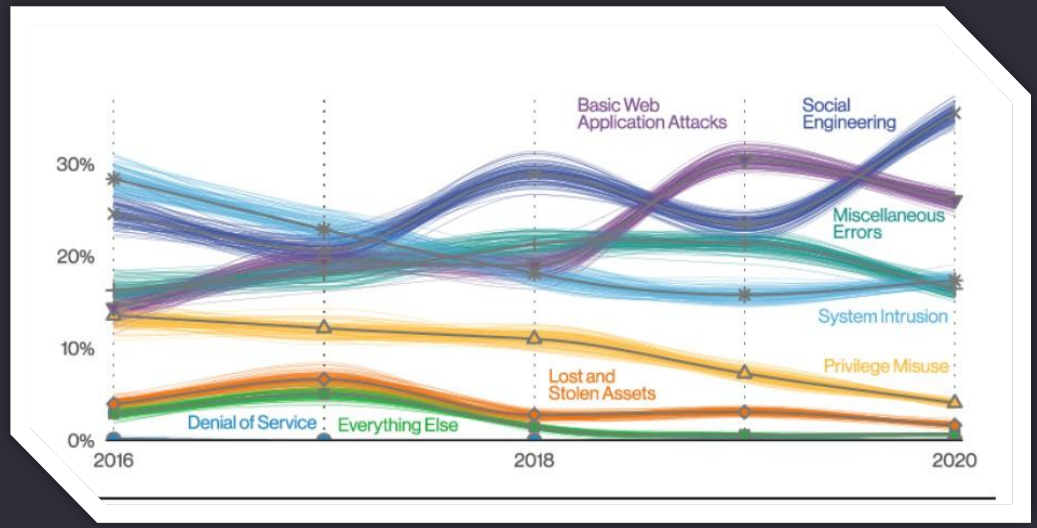
Cyber risks are here to stay

Ransomware has continued its upward trend with an almost **13% rise** an increase as big as the last **5** years combined.

It's important to remember that while ubiquitous and potentially devastating, ransomware by itself is, at its core, simply a model of monetizing an organization's access.



The **human element** continues to drive breaches. Whether it is the use of stolen credentials, phishing or simply an error, people continue to play a large part in incidents and breaches alike.



SOURCE: https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

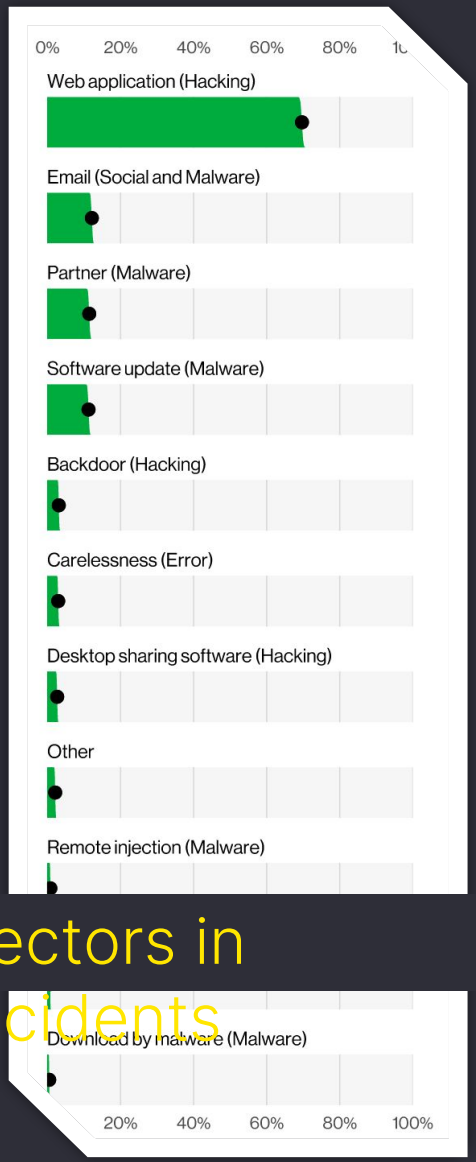
The top questions for consideration

1	2	3	4	5
Is Cyber managed with an assumed breach mindset?	Are you managing critical third parties as an exposed supply chain	Do you have capability to detect, respond, recover and communicate when a Cyber Incident happens?	Do you have a Cyber Response Plan?	When was the last time you tested the Cyber Response Plan?

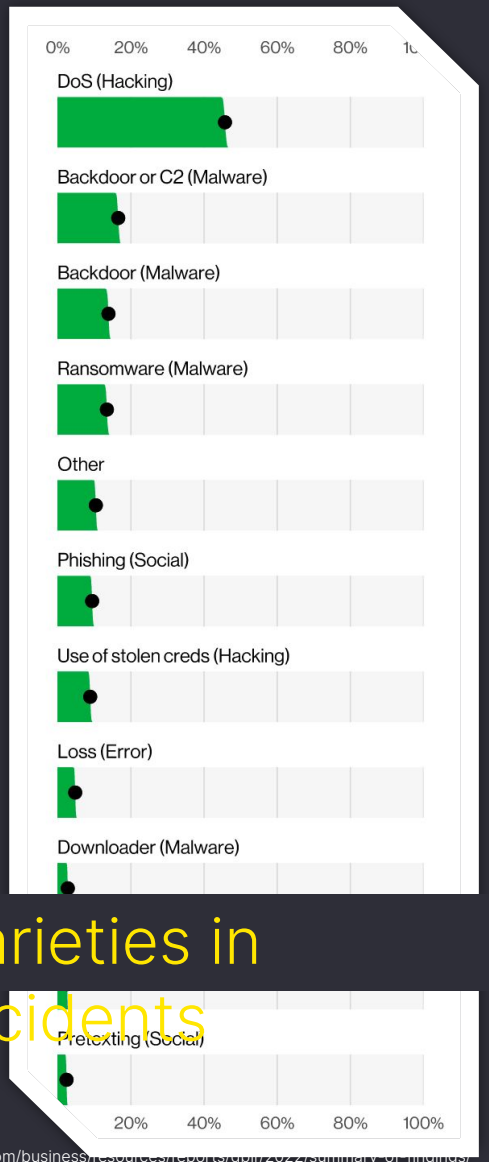
What does cyber resilience really mean?

Ability to stop an Incident from turning into a Breach.

In terms of vectors, the main ways in which a businesses are poised for growth as part of their digital imperative is the manner in which they are exposed and are vulnerable.



Vectors in Incidents

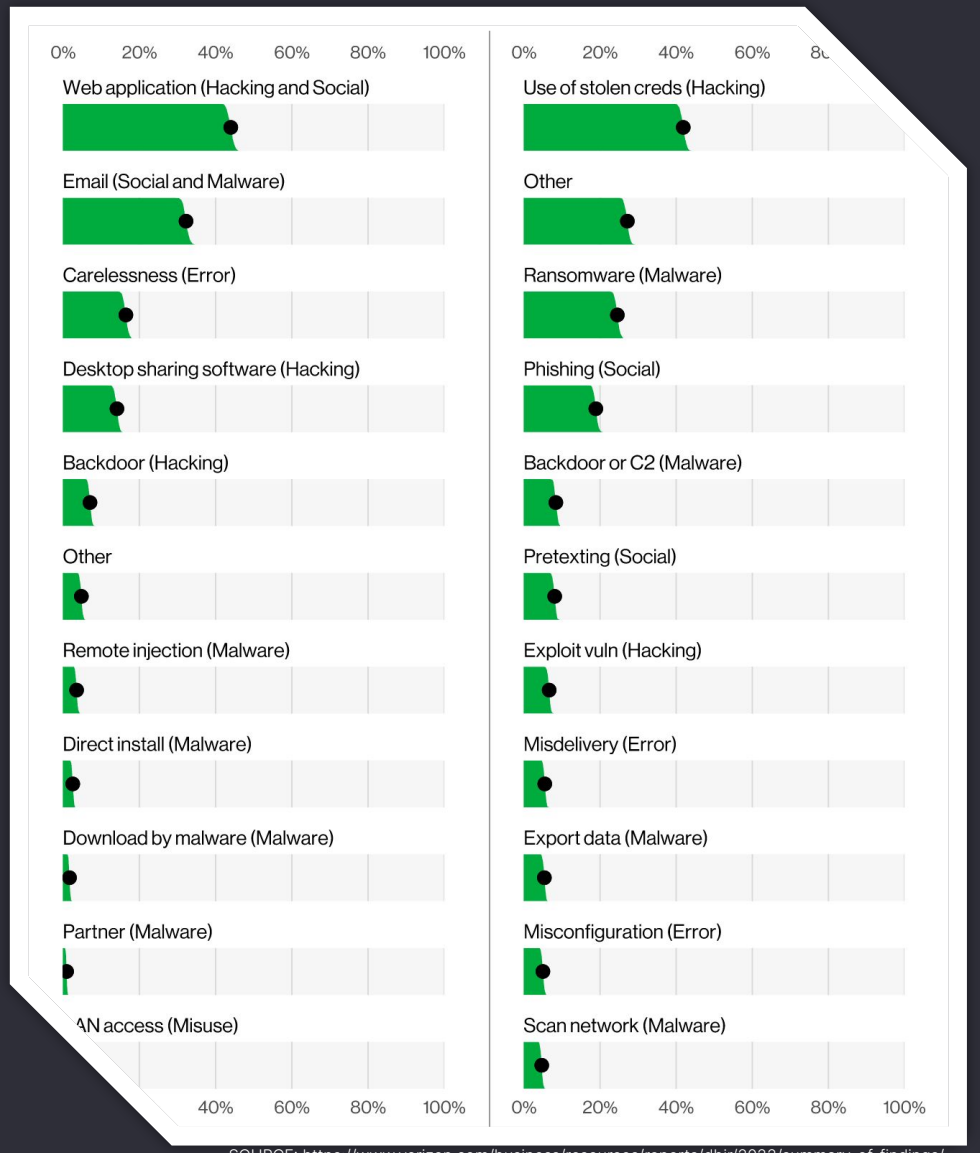


Varieties in Incidents

SOURCE: https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

Top 5 compromise types are still the same

1. Web Applications
2. Email Compromise
3. Social Engineering
4. Stolen Credentials
5. Phishing



SOURCE: https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[2013 DBIR page 31]"

"The first case of Ransomware showed up in our data in 2008 and it wasn't until 2013 that we had sufficient data to write something about it. And we quote:
...When targeting companies, typically SMBs, the criminals access victim networks via Microsoft's Remote Desktop Protocol (RDP) either via unpatched vulnerabilities or weak passwords. Once they've gained initial access they then proceed to alter the company's backup so that they continue to run each night but no longer actually backup any data. [2013 DBIR page 31]"

The ever-increasing count of cyber challenges

- Identity security
- Privacy
- Infrastructure posture
- Trust based communication
- Data accuracy and security
- Third parties and their ecosystems
- Elastic Network
- Management of multiple platform
- Hardware and device security
- Devices linked to your environment
- Cloud ecosystems
- Infiltration into software and hardware
- Responsibility for securing BYOT
- Authentication and Accountability
- Privileged account management
- Executive mindset
- Lack of funding
- Rapid technology changes
- Skills shortage
- Lack of funding

Where to focus?

How to action a Cyber Resilience approach

1	2	3	4	5
Take a data centric approach to securing your assets	Re align your readiness to a threat based model and understand active threat actors	Build safe guards to ensure humans as the last line of defence is not compromised	Secure the third party supply chain	Continuously assess your response readiness with an assumed breach model

Cyber resilience approach to deal with emerging threats

October 2022

Puneet Kukreja
EY Ireland (UKI) Cyber Leader

Building a better working world

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 003145-22Gbl
ED None

ey.com