HealthHub Connect

Executive Presentation

PRACTERA – TEAM 2

AGENDA

- *A global summary of the top cyber risks facing all businesses for 2023/24*
- *An analysis identifying specific risks faced by companies in one or more sectors that HealthHub Connect operates*
- *A case study on a recent cybersecurity incident faced by a competitor or comparator to HealthHub Connect*
- *A vulnerability scan and report for the website*

Global Summary

11 Global Cyber Risk

2023/2024

Cyber Risks for Global Businesses:

1. *Vulnerability*
2. *Privacy Breaches*
3. *Phishing*
4. *Ransomware*
5. *Social Engineering*
6. *State - Sponsored Attack*
7. *IOT Attacks*
8. *Risky Remote Work Environments*
9. *Mobile Attacks*
10. *Cyber-physical attacks*
11. *Cybersecurity Professionals Shortage*

Vulnerability:

Flaws in a computer system that weaken the overall security of the device either in the hardware itself or the software that runs on it

Privacy Breaches:

The loss of control, compromise, unauthorized acquisition, or any similar occurrence where an unauthorized person accesses a data or use for unauthorized purpose

Phishing:

The practice of sending fraudulent communications that appear to come from a legitimate and reputable source, usually through email and text messaging.

Ransomware:

a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files for a ransom

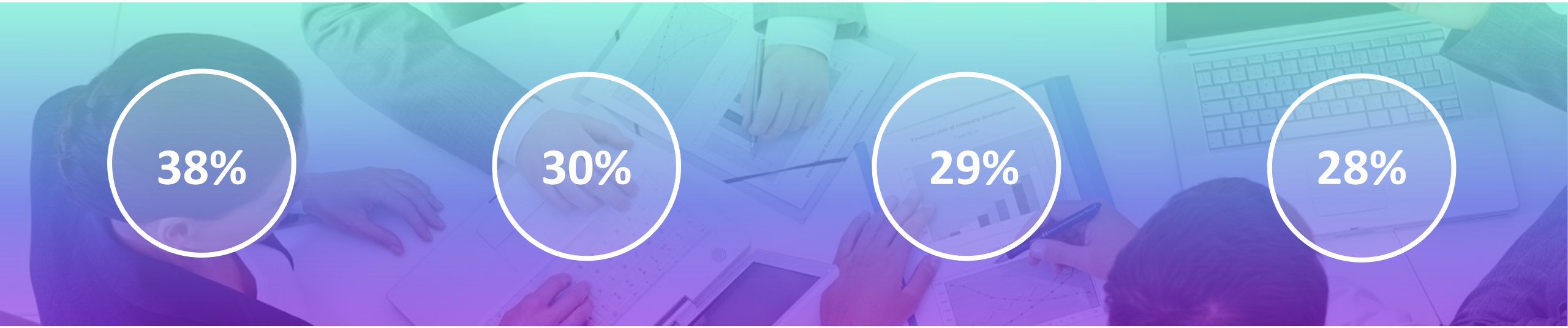
Social Engineering:

a way of using IT technologies as support to psychological manipulation techniques to achieve an objective outside the IT realm

State-sponsored Attack:

are cyber attacks supported by governments or its agencies against other nations, organizations or individuals. It's a way to promote a nation's interest at home or abroad

Global Summary
– What has made professionals' job more difficult



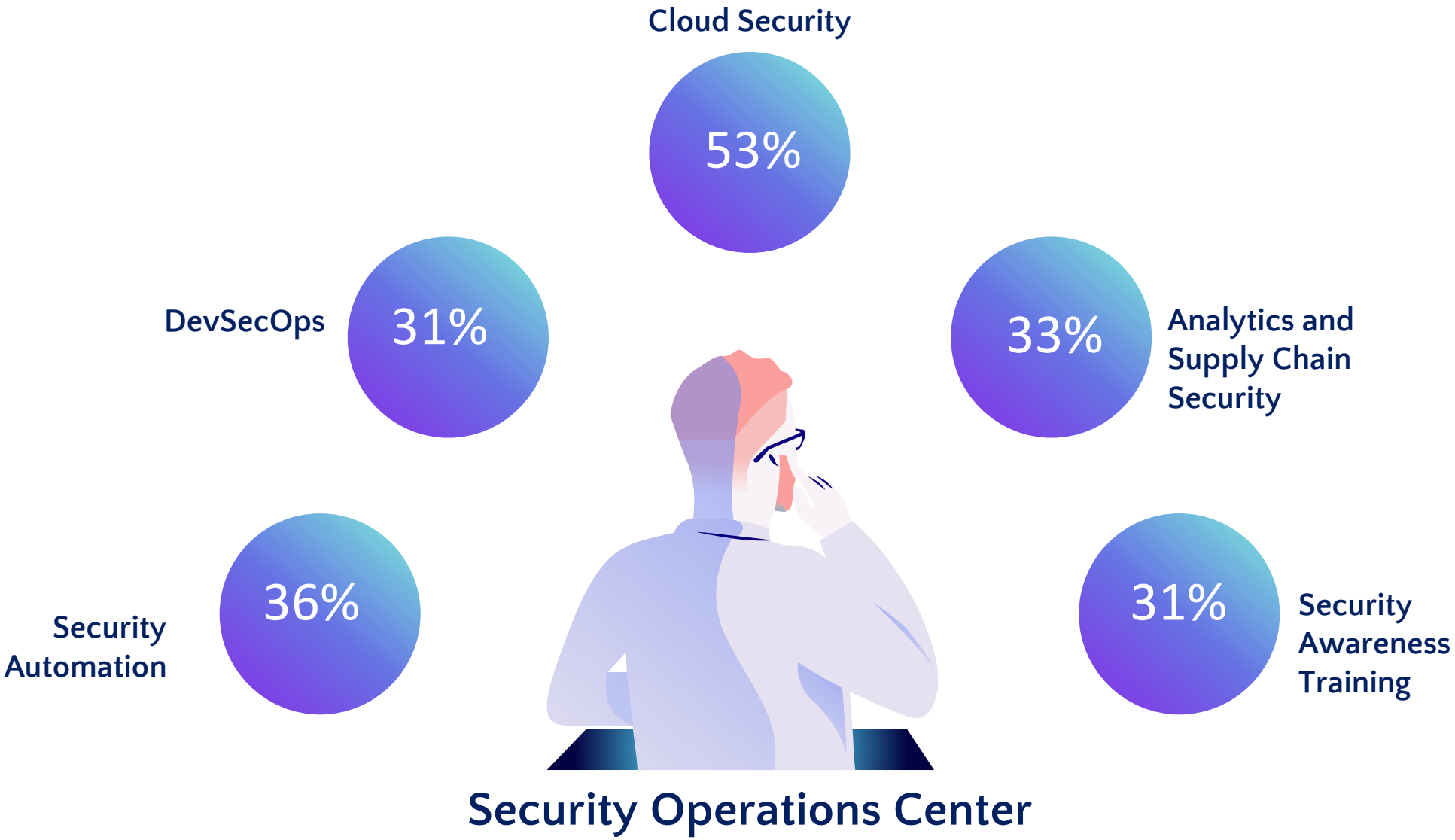
The increasing sophistication of threats

Security stack complexity

Iaas and SaaS driving challenges in risk monitoring and management

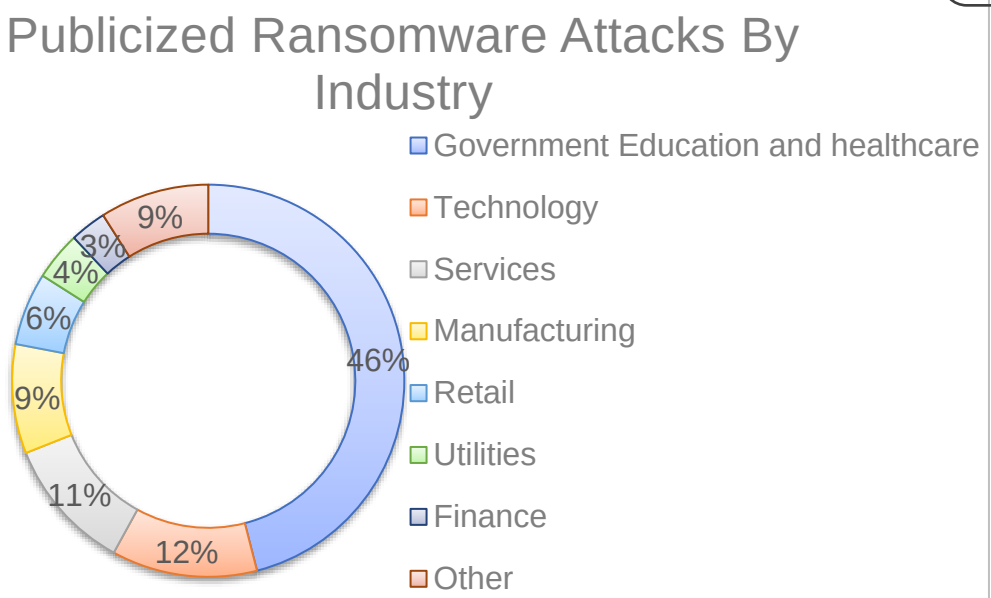
Workload demands trapping teams in "react mode"

Global Summary
- Top Security Initiatives



Health Insurance-Tech: Vulnerable Sector for Cyber Attacks

Insurance sector has a lot of personal information of their clients', which make sit the favorite sector for hackers to steal data from



PII Records:

- *PII Data held by insurance companies can be exploited by thieves for fraud.*
- *Dates of birth and Social Security numbers are the most significant PII data points.*
- *These are essential components of identity theft schemes like fictitious credit applications.*

Ransomware attacks:

- *Ransomware operators can get policy details and security standards for their insurance customers through network compromises.*
- *Huge amount of ransom can be demanded for such kind of data*

PHI Records:

- *Most sensitive data among personal data*
- *Categories can be used against a person for unethical reasons*
- *Consequently, information on Medicare and Medicaid coverage is a highly sought-after commodity in these underground criminal markets.*

Financial Impacts and Infrastructure challenges

Financial Cost of Cyberattacks

$600k *Average payment for Ransomware hijack in US*

$20 Bn *Ransomware cost to the US per year*

Infrastructure challenges contributing to increase in cyber attacks

- *Companies that continue to use software after support has been withdrawn by the developer are three times more likely to make a cyber claim.*
- *Vulnerabilities in the information system still pose a big threat to information security. 25096 vulnerabilities were reported by US government in 2022.*
- *Consistent attacks by hackers.76% of cyber attacks are contributed by Phishing alone. One employee's mistake can cost millions of dollars in damage. It has increased by 30% since 2022.*

Case Study

Sun Life Data Breach (MOVEit cyber incident) - June 2023

Company Description:

Sun Life is a Canadian-based financial services company that provides solutions including health insurance, and asset management for individuals and businesses.

Data Breach:

Sun Life experienced a data breach caused by a third-party vendor's use of the MOVEit file transfer software, which was exploited by the Clop ransomware group.

Incident Overview:

One of the Sun Life vendors, Pension Benefit Information, LLC (PBI), advised to customers in late June 2023 that one of its servers was accessed by an unauthorized third party as part of the global attack.

Because of this, some U.S. personal member's information of Sun Life shared with PBI to support their business was accessed by some unauthorized party. PBI advised that they were not aware of any indications of identity theft or fraud in relation to this event.

Case Study

Impact:

The data breach impacted 212,129 individuals, whose personal information was accessed by unauthorized third parties. PBI confirmed that personal information accessed by hackers included name, Social Security Number, policy/account number and/or date of birth of some members and account holders.

Investigation:

As a part of investigation, Sun Life took information security very seriously and conducted their own investigation alongside PBI to confirm what data was involved. Working along with PBI, they notified members whose personal information was affected.

Timeline:

In June 2023, Sun Life experienced its first data breach caused by a third-party vendor's use of the MOVEit file transfer software, which was exploited by the Clop ransomware group.

Vulnerability:

The reason for the attack is not clear. Sun Life conducted its own investigation alongside the vendor, Pension Benefit Information (PBI), to confirm what data was involved and notified members whose personal information was affected.

Case Study

Lesson Learned:

Sun Life provided any applicable free credit monitoring and identity theft restoration services and also encouraged members to take precautions such as monitoring their accounts and credit history for signs of unauthorized activity, along with other ways to protect their information.

Regulatory Implications:

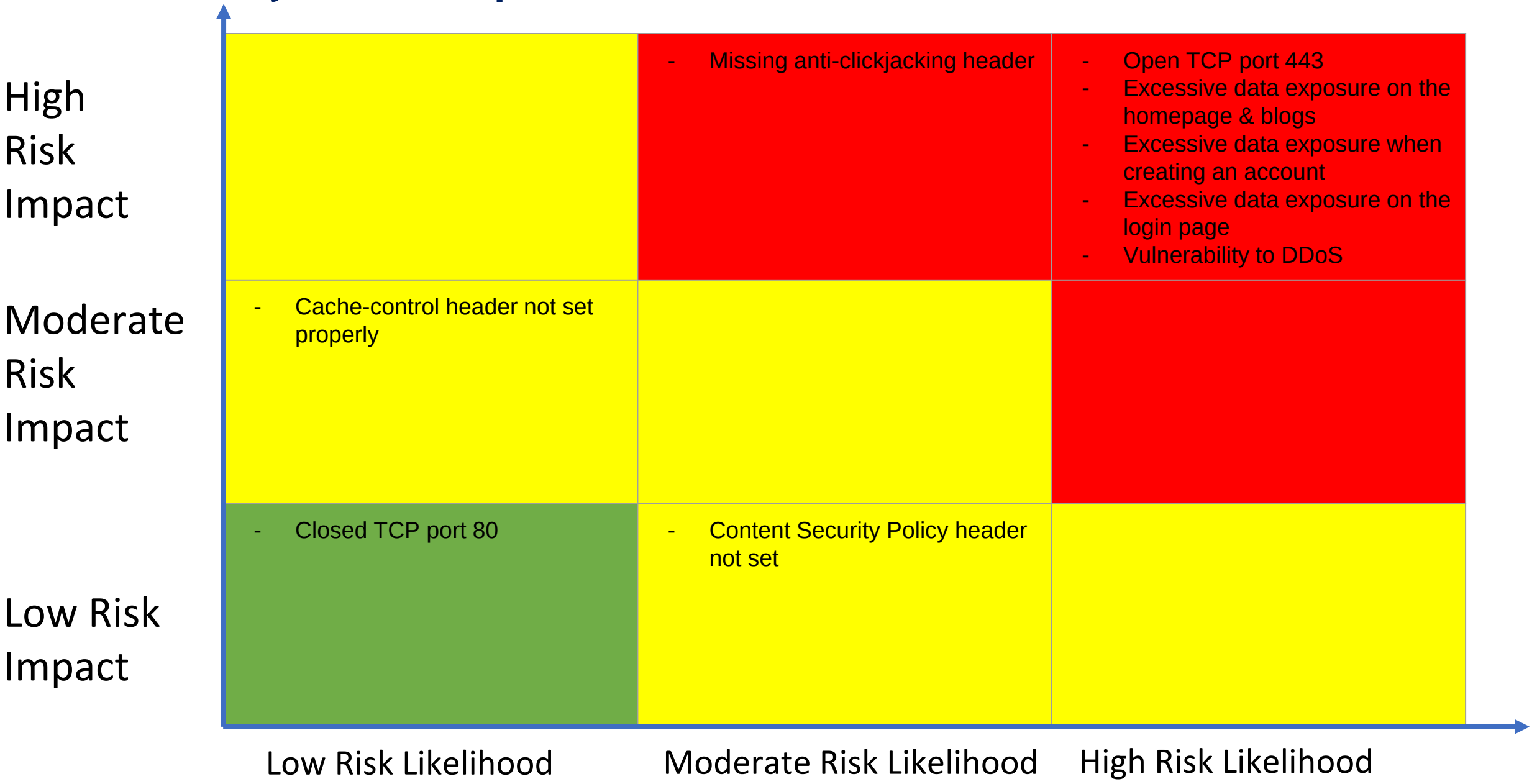
Due to the data breach, lawyers are eager to speak to victims of the Sun Life to determine what damages they sustained and what compensation may be available to them. Sun Life provided free consultation to discuss about legal options for whoever received a NOTICE OF DATA BREACH.

Prevention:

Sun Life use powerful security safeguards to protect customer information when they visit company websites and when they communicate with customers and use strong safeguards like:

- *Data encryption and message Integrity*
- *Authentication of customer identity*
- *Password protection*
- *Session Time-out.*

Vulnerability Scan Report On The Website



Thank You

Practera Team 2 - 2024