unimutual

Cyber Webinar

Security ScoreCard

13th May 2021

Presenters

Max Broodryk

Product Leader – Cyber Risk
International Financial Lines

AXA

Richard Head

Principal

headsure

Tim Geschwindt

Senior Incident Responder
Senior Analyst

S-RM

Learning Objectives

1. Understand The Escalating Global Cyber Threat Environment

2. Understand The Insurance Market Response To Escalating Risk

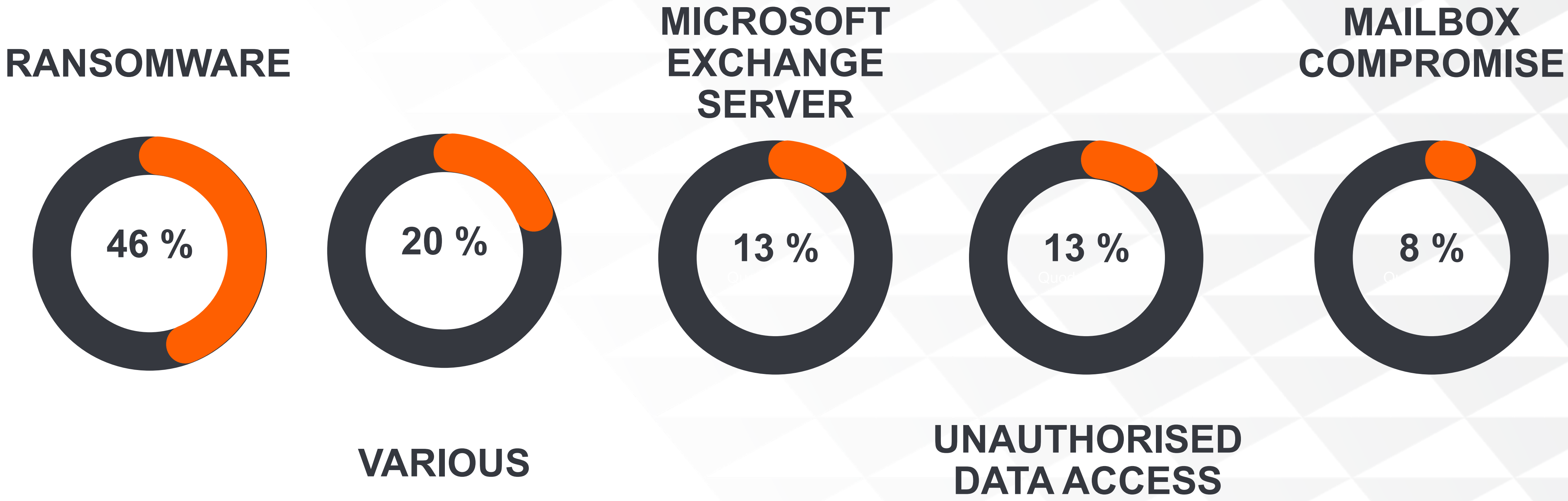
3. How To Use Security Scorecard To Identify & Mitigate Cyber Risk

The Cyber Threat Landscape

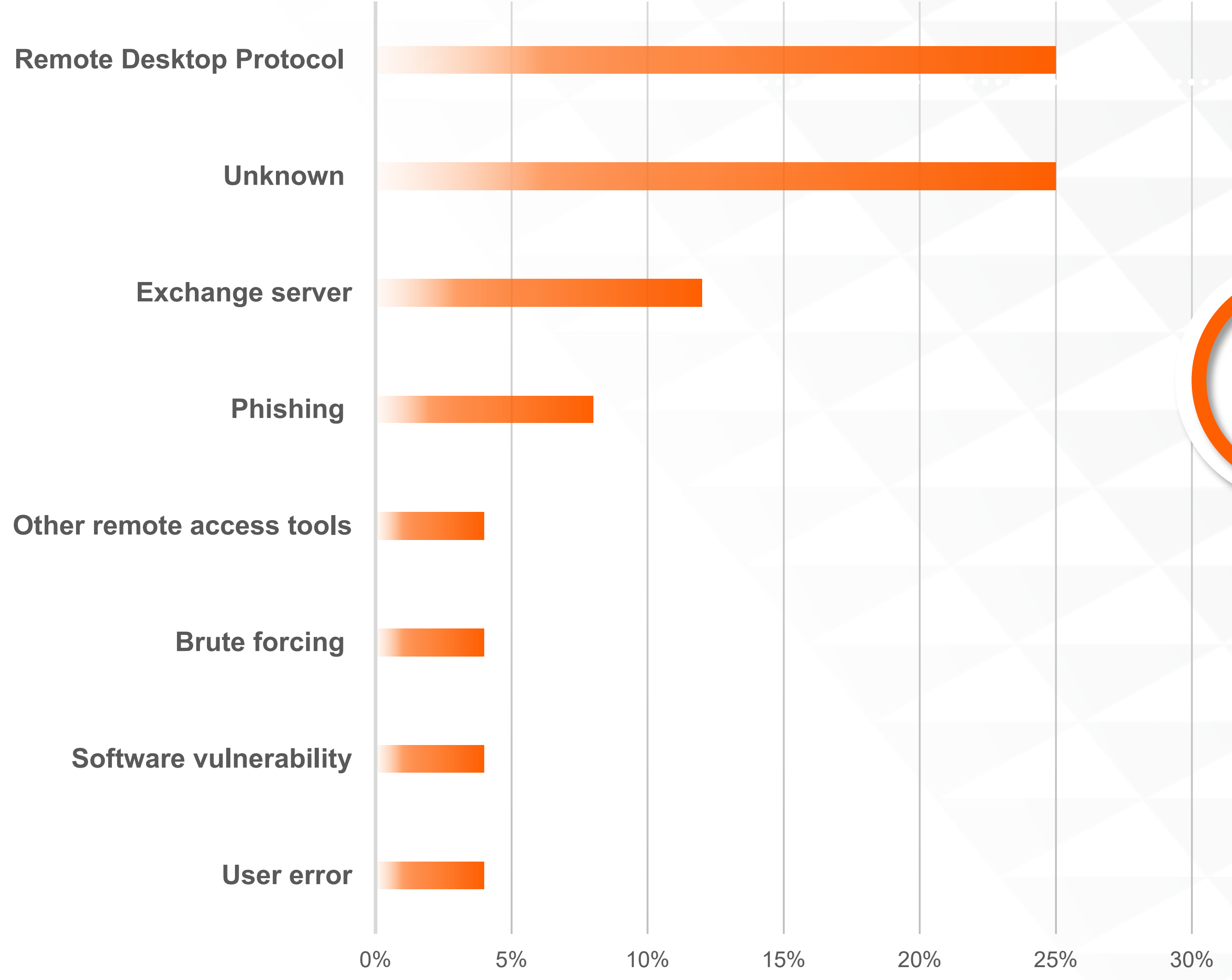
The Picture From Q1

Types of Incidents

103 Incidents Since 1 Jan 2021



How Do They Get In?

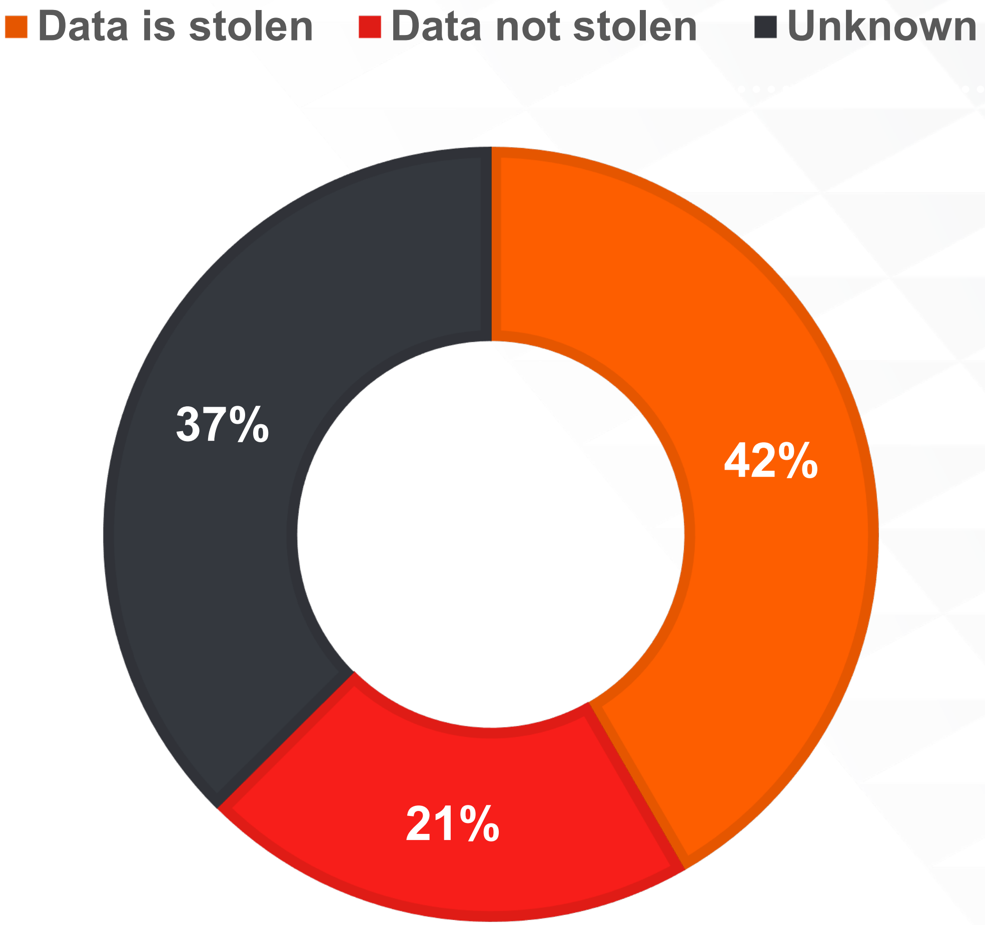


STEP 1

INTRUSION

S-RM

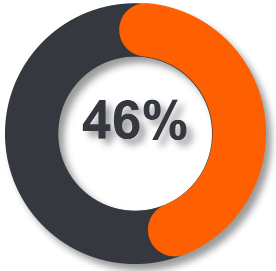
How Often Is Data Stolen?



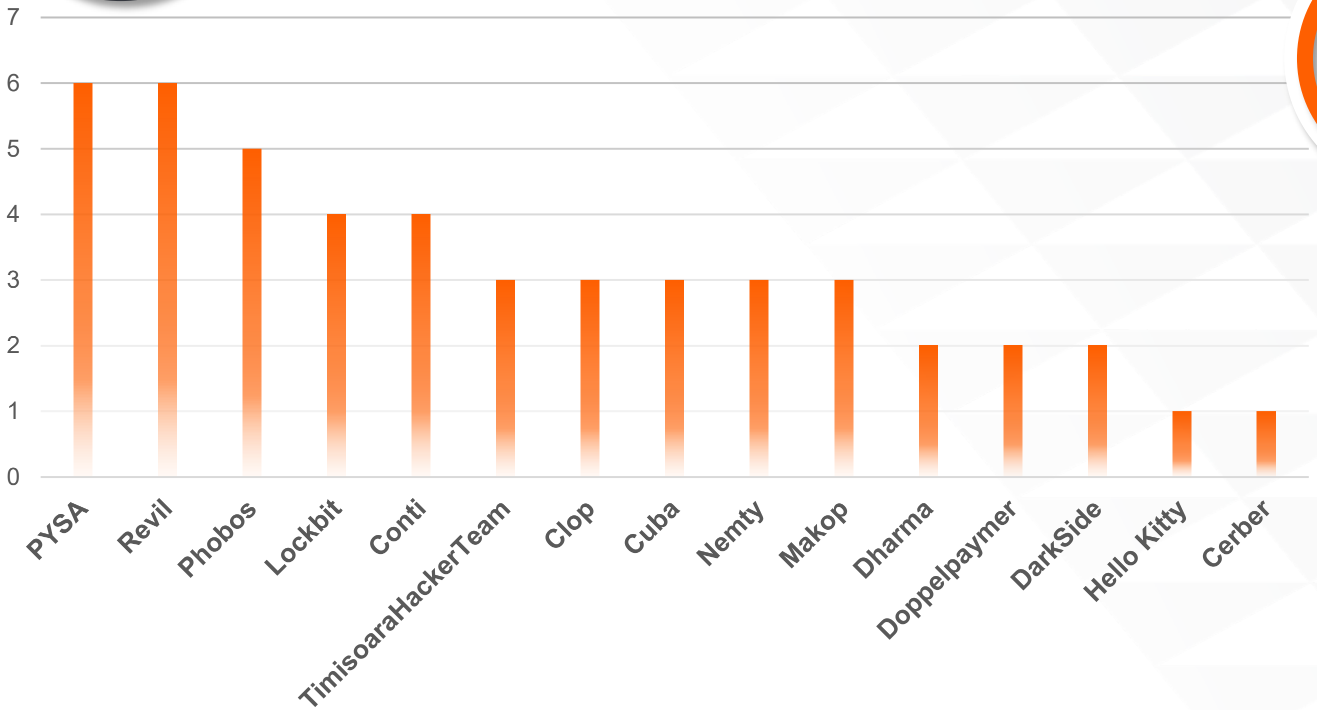
STEP 2

DATA THEFT

How Often Is Data Held To Ransom?



Threat actors are holding encrypted data for ransom in 46% of cases



And By Whom?

STEP 3

RANSOMWARE

S-RM

How Often Are Ransoms Paid?

And How Much?

A ransom was paid in

16 %

of S-RM cases

The ransom negotiation rate was

57 %

on average

In one case we negotiated the ransom down

89 %

from USD 2.5 million to 300,000

STEP 4

RANSOM NEGOTIATION

Overall Trends

1 Increasing frequency of incidents, especially ransomware

2 Rapidly evolving methodology

3 Extortion on the risk across all attack types

4 Increasing sophistication and organisation

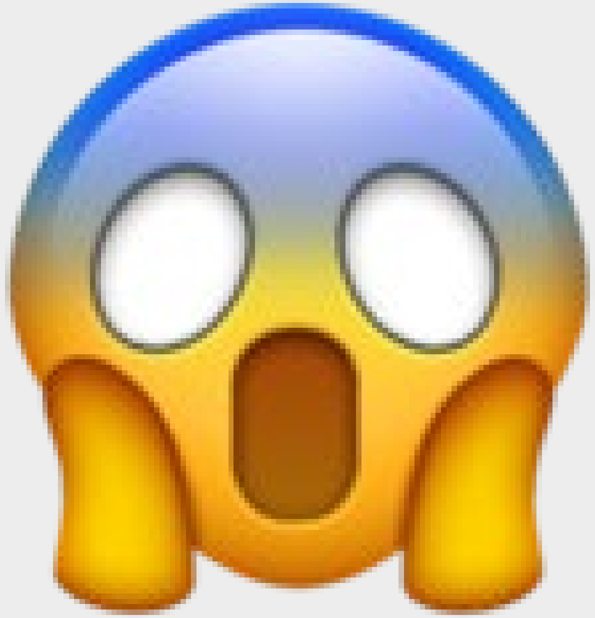
headsure

Cyber Insurance Market

A Response to Risk

Losses Mounting, Fear Rising

- Significant Large Losses
- Insufficient Premium Pool
- Difficult Risk to Price
- Claims Costs Increasing
- Fears of Systemic Risk
- Pandemic Tailwind
- Increased Regulatory Risk
- Low Returns, High Reinsurance Costs



Insurer Behaviour is Changing

- ➢ Exit or Remediate
- ➢ Focus on Risk Selection
- ➢ More Information
- ➢ Risk Assessments
- ➢ Restrict Capacity
- ➢ Limit Cover
- ➢ Increase Premium
- ➢ Increase Retention

The AXA XL Perspective

Max Broodryk

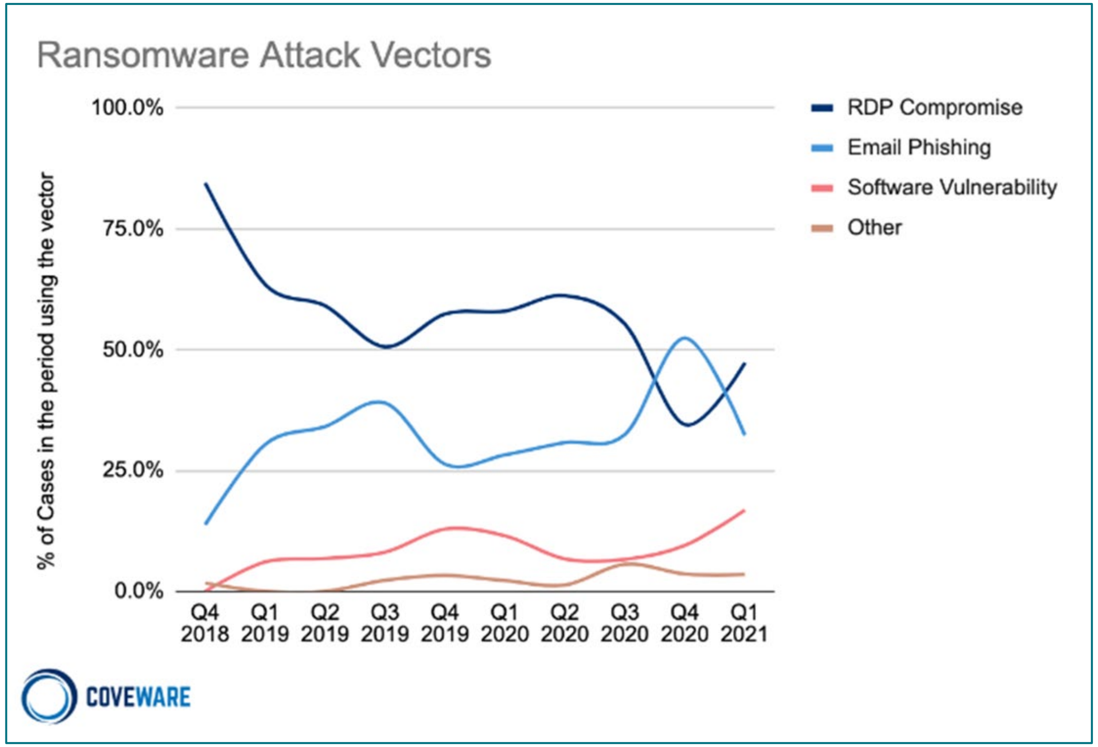
Product Head, Cyber Risk

May 2021

AXA XL Perspective

Preventing a ransomware attack

- Multi-factor authentication
- Phishing Training / awareness
- Patching
- Vulnerability scanning / penetration testing



AXA XL Perspective

After being attacked….

…mitigation of loss

- Secure administrator accounts
- Monitoring 24/7

…response and recovery

- Crisis Plan
- Back-ups (offline, tested)

AXA XL Perspective

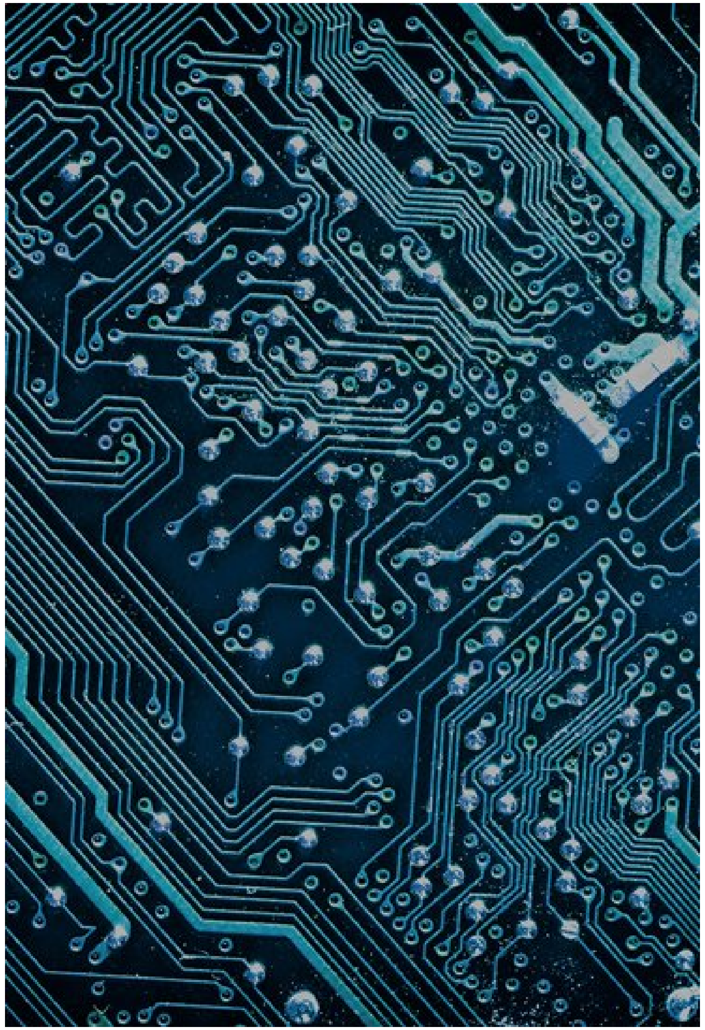
Security Scorecard

-

- Security Scorecard is “outside in”
- Can’t identify or measure everything that matters
- Potential for false positives that affect scoring.

+

- Independent / standardized
- Allows benchmarking against peers
- Simplifies complexity
- Allows risk management conversations across business functions and entities

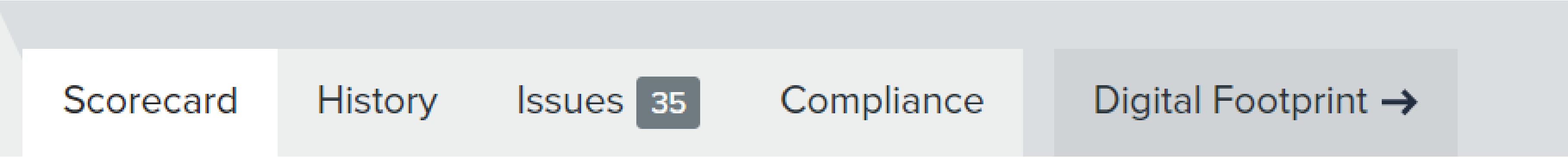


Security Scorecard

What Does The World See

What Is Security Scorecard (SSC)

- Platform that collects, attributes and scores the overall cyber security health of an organisation
- Scans for common vulnerabilities, exposed services and poor cyber hygiene
- It is a passive vulnerability assessment tool which gives an insight into the security posture of an organisation over time



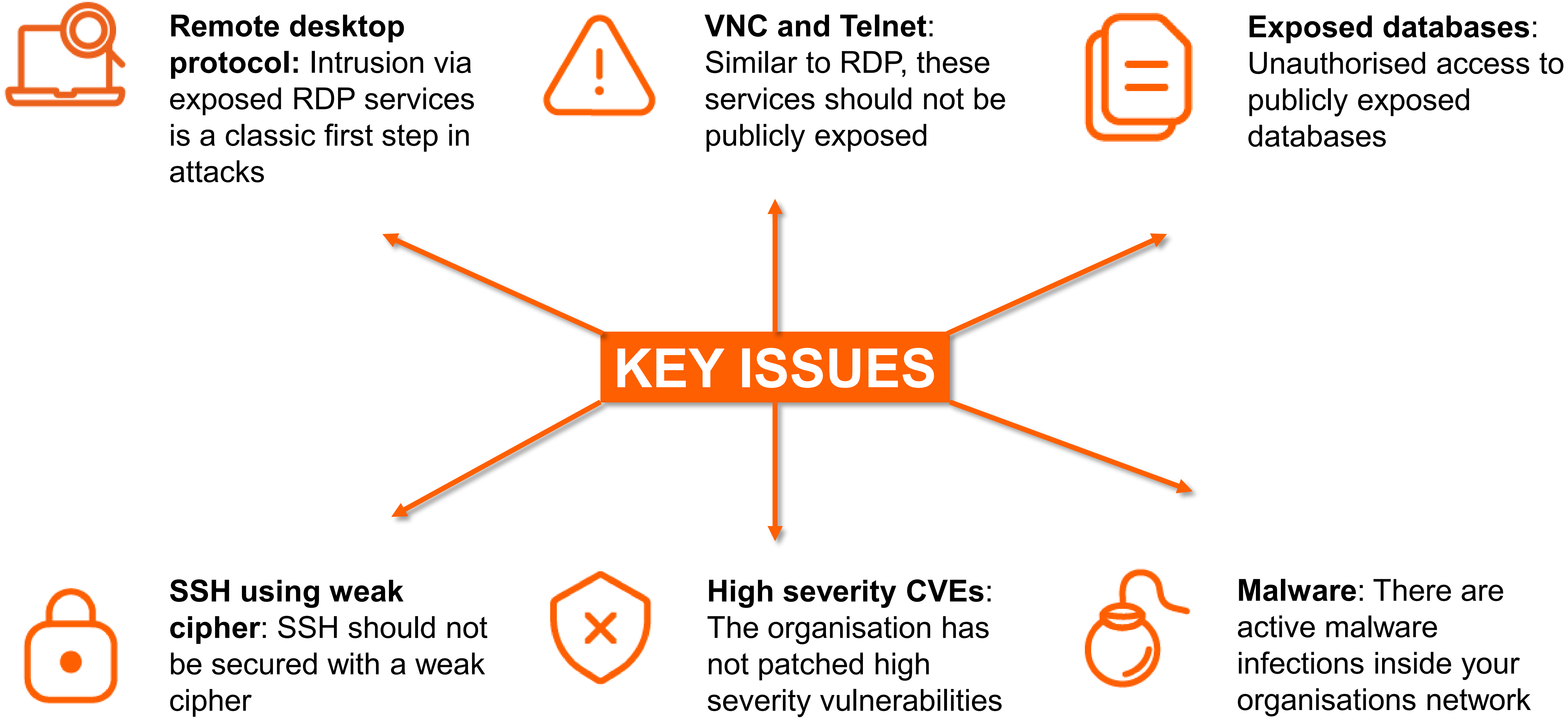
S-RM

What Does It Cover?

Control area
Network security
DNS health
Patching cadence
Endpoint security
IP reputation
Application security
Cubit score
Hacker chatter
Information leak
Social engineering

How Is It Rated?

Letter grade	Numeric score
A	90 – 100
B	80 – 89
C	70 – 79
D	60 – 69
F	0 – 59



KEY ISSUES

Remote desktop protocol: Intrusion via exposed RDP services is a classic first step in attacks

VNC and Telnet: Similar to RDP, these services should not be publicly exposed

Exposed databases: Unauthorised access to publicly exposed databases

SSH using weak cipher: SSH should not be secured with a weak cipher

High severity CVEs: The organisation has not patched high severity vulnerabilities

Malware: There are active malware infections inside your organisations network

Validating Findings

Digital Footprint

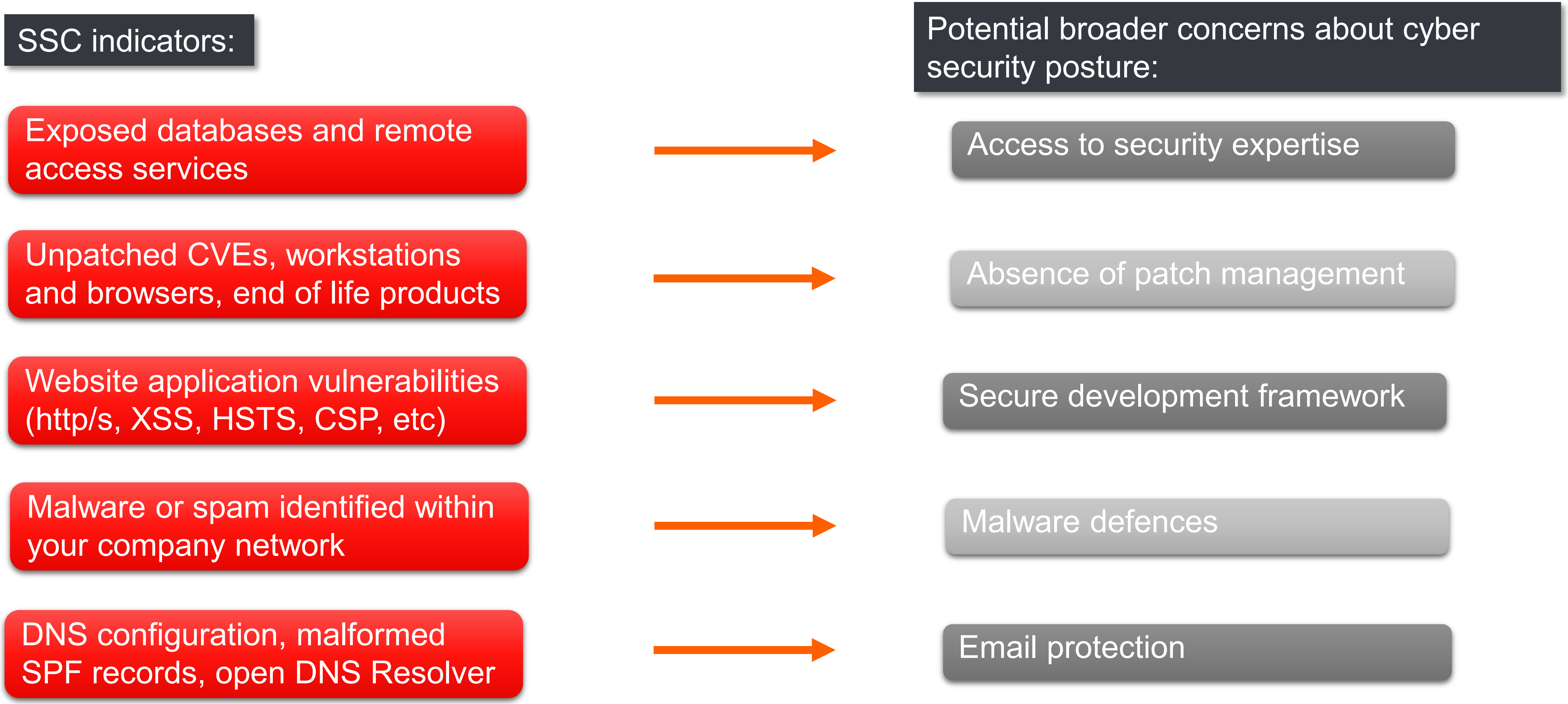
- A company's digital footprint is compiled automatically
- Check IP ranges for accuracy
- Check domains and sub-domains for accuracy
- If this is inaccurate, you can submit the correct IPs and domains

False positives

Evaluate the 'Issues' tab for false positives, such as:

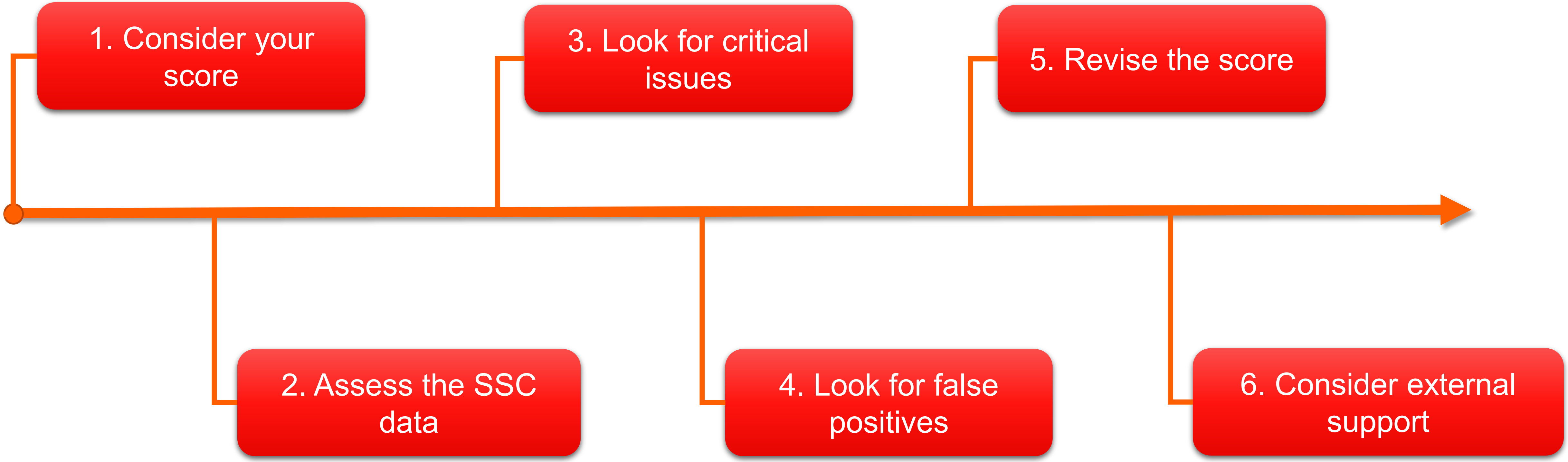
- Outdated OS and browsers: Check whether these outdated OS's and browsers are on devices operating on a guest network
- Missing HTTPS: Check whether the site in question needs HTTPS. If it does not host content it may not need this security feature.

Beyond The Score, What Does This Mean

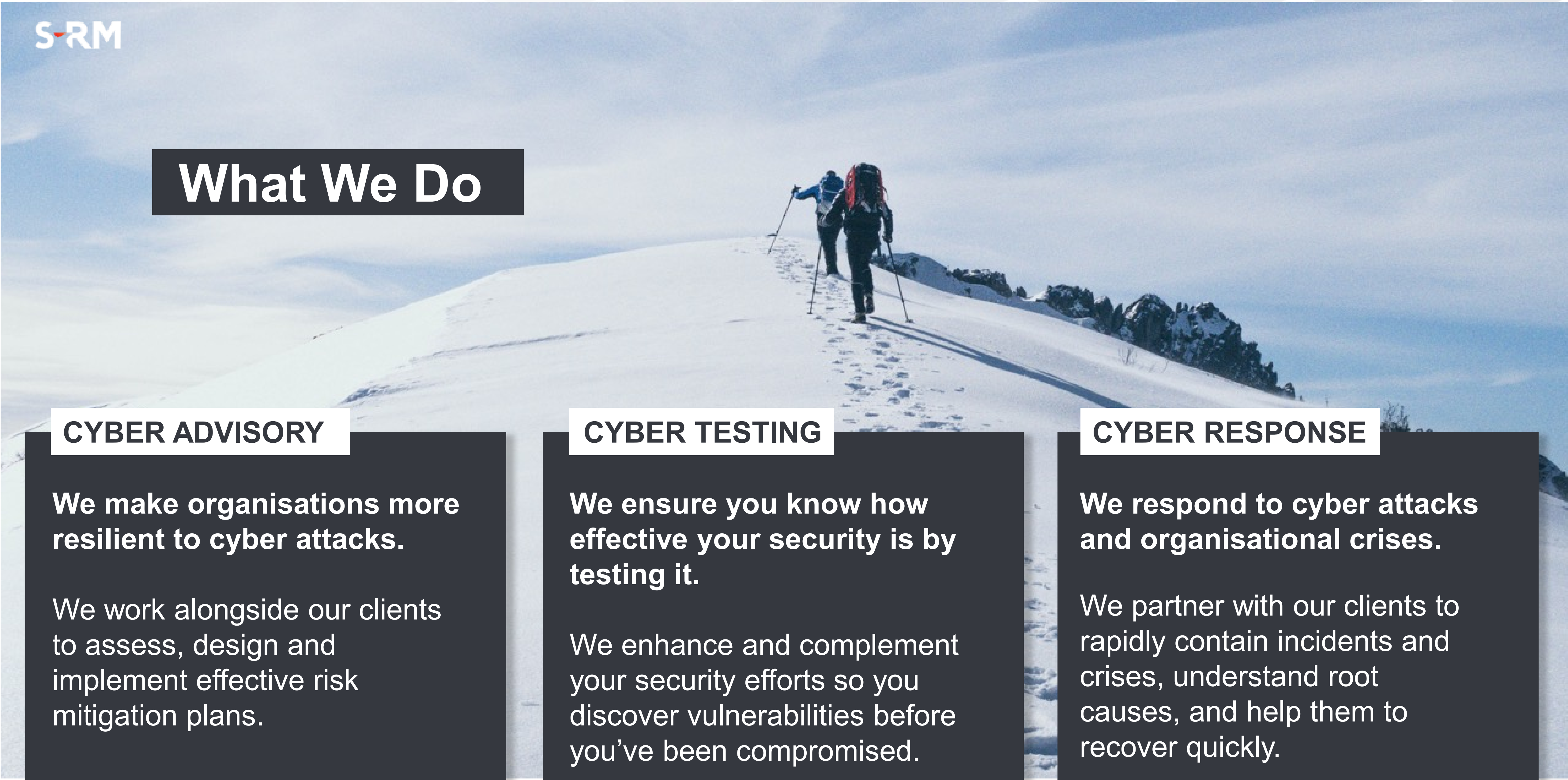


SSC indicators:	Potential broader concerns about cyber security posture:
Exposed databases and remote access services	Access to security expertise
Unpatched CVEs, workstations and browsers, end of life products	Absence of patch management
Website application vulnerabilities (http/s, XSS, HSTS, CSP, etc)	Secure development framework
Malware or spam identified within your company network	Malware defences
DNS configuration, malformed SPF records, open DNS Resolver	Email protection

Wrapping Up



1. Consider your score
2. Assess the SSC data
3. Look for critical issues
4. Look for false positives
5. Revise the score
6. Consider external support



What We Do

CYBER ADVISORY

We make organisations more resilient to cyber attacks.

We work alongside our clients to assess, design and implement effective risk mitigation plans.

CYBER TESTING

We ensure you know how effective your security is by testing it.

We enhance and complement your security efforts so you discover vulnerabilities before you've been compromised.

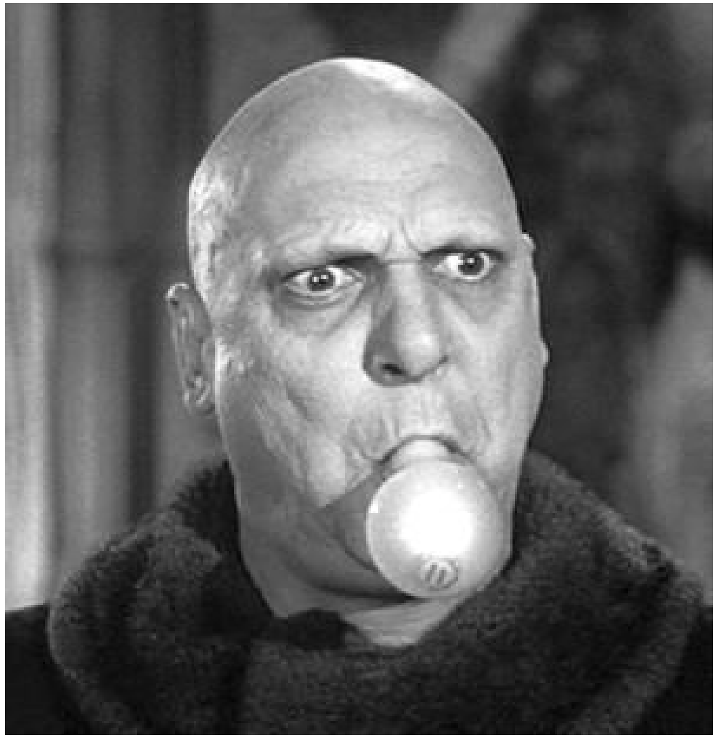
CYBER RESPONSE

We respond to cyber attacks and organisational crises.

We partner with our clients to rapidly contain incidents and crises, understand root causes, and help them to recover quickly.

Key Takeaways

- Increasingly Hostile Cyber Threat Environment
- Straining the Global Cyber Insurance Market
- Top Down Approach to Mitigating Cyber Risk
- Security Scorecard Can Assist
- Provide IP Addresses & Contacts
- Work on Improving Your Score



Questions

unimutual

For more information, please contact us:

Christine Cummings
(For memberships)

(02) 9250 2806

+61 423 204 040

christine.cummings@unimutual.com.au

Jamie Thomson
(For claims)

(02) 9250 2807

+61 431 473 156

jamie.thomson@unimutual.com.au

Salinda Saat
(For underwriting)

(02) 9250 2824

+61 436 379 009

salinda.saat@unimutual.com.au

Thank You

Unimutual Limited
Suite 11.02, Level 11,
56 Pitt Street, Sydney NSW 2000

Phone: (02) 9247 7333
Fax: (02) 9252 9070
Email: service@unimutual.com.au
Website: www.unimutual.com

ABN: 45 106 564 372 / AFS Licence No: 241142