# The CFO’s Role in Building Cyber Resilience

## Palo Alto Networks

8 November 2024

# Palo Alto Networks at a glance

**Largest standalone cybersecurity company** (>$8B in global FY24 revenue, 20% in EMEA)

**>15,000 employees**

**~$10B spent on innovation in last five years** (1)

**Externally recognized leadership across 24 cybersecurity product areas**

(1) Non-GAAP R&D expense + M&A consideration for FY20-FY24

# Palo Alto Networks Product and Service Offerings

## Network Security

**STRATA**

Best-in-class security delivered across hardware, software and SASE

## Cloud Security

**PRISMA CLOUD**

Comprehensive platform to secure everything that runs in the cloud

## Security Operations

**CORTEX**

A new approach to SOC with fully integrated data, analytics and automation

## Threat Intelligence and Advisory Services

World-renowned threat intelligence, cyber risk management and advisory services

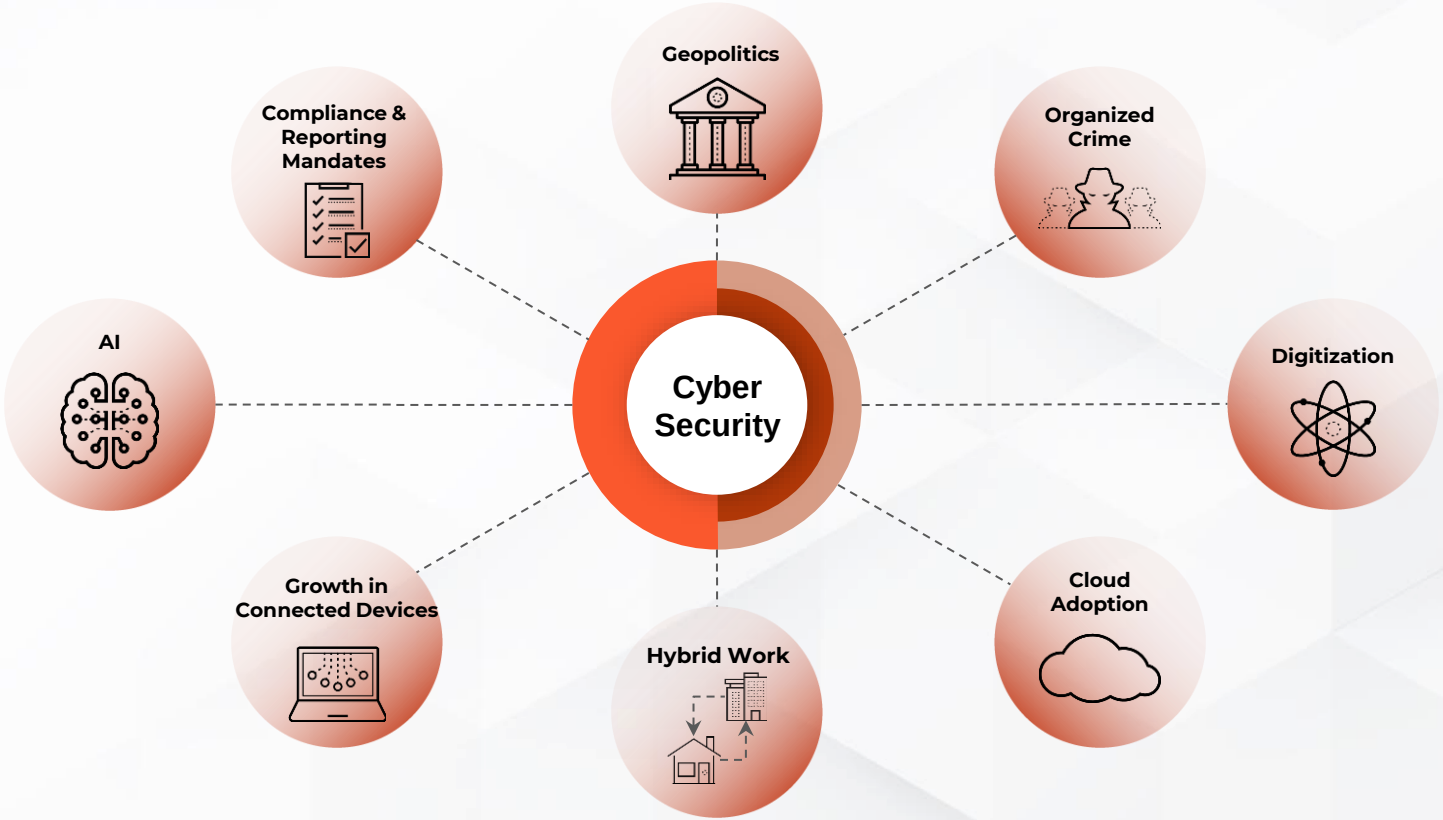
# Cyber risk is #1 identified risk in 2024 and fueled by significant forces

| Most significant business risks in 2024 (per Allianz) | |
|---|---|
| **Rank** | **Risk scenarios** |
| **1** | **Cyber incident** |
| 2 | Business interruption |
| 3 | Natural catastrophe |
| 4 | Changes in legislation & regulation |
| 5 | Macroeconomic developments |
| 6 | Fire, explosion |
| 7 | Climate change |
| 8 | Political risk & violence |
| 9 | Market developments |
| 10 | Shortage of skilled workforce |

Sources: Allianz Risk Barometer 2024 report,

# Inter-related set of drivers fueling cybersecurity risk

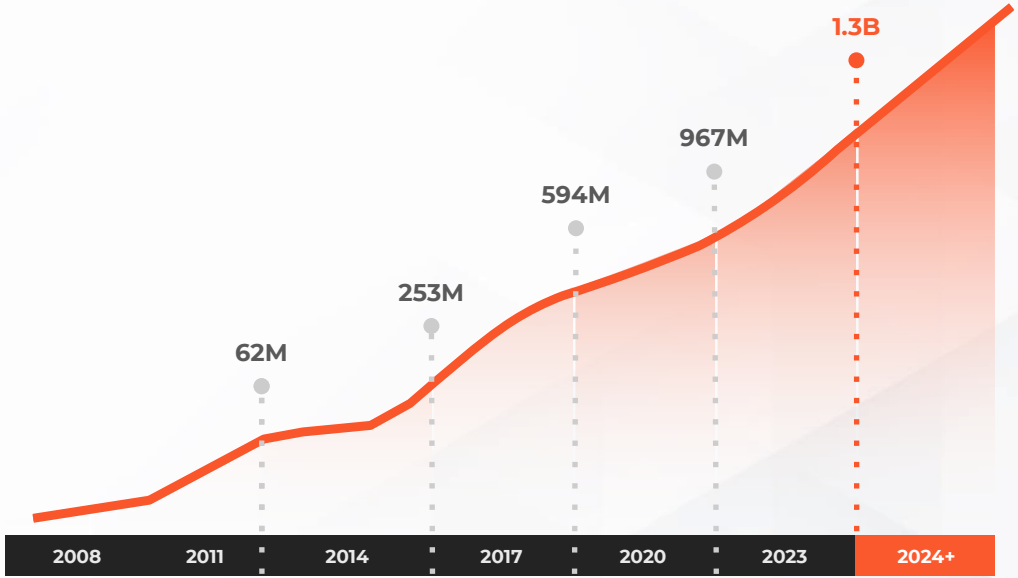



Sources: Statista; MIT Technology Review; Palo Alto Networks "What's Next in Cyber" survey 2022, Business Value Consulting analysis

# Malicious activity is on the rise; AI is beginning to fuel this

## 20x increase in malicious programs since 2011[1]




## The attackers are already leveraging AI

Bypassing **identity checks**

Generating **deepfakes**

Leveraging **LLMs** for malicious intent

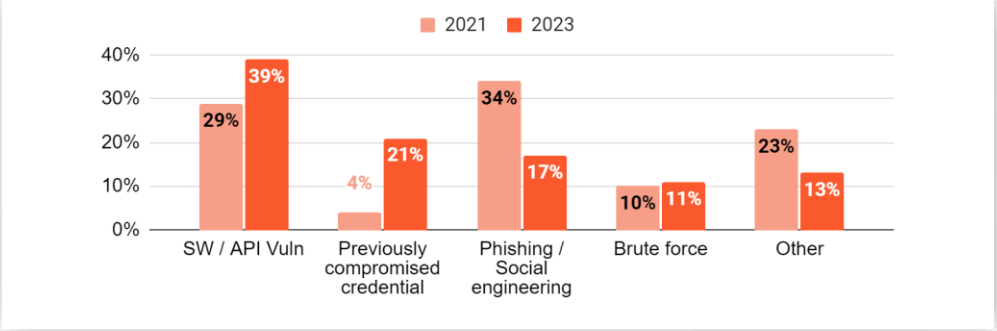
Sources:
[1] https://portal.av-atlas.org/malware.

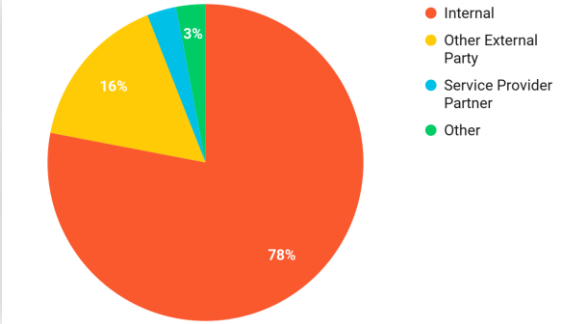
paloalto NETWORKS

# The state of cyberattacks

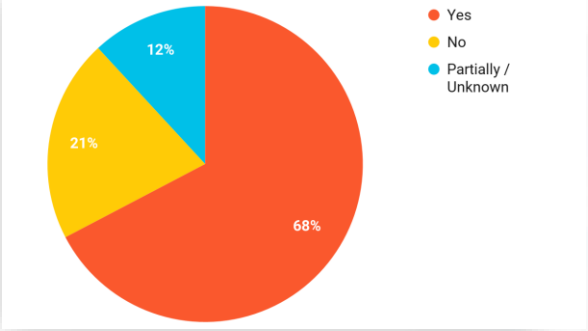
## How do attackers get in?



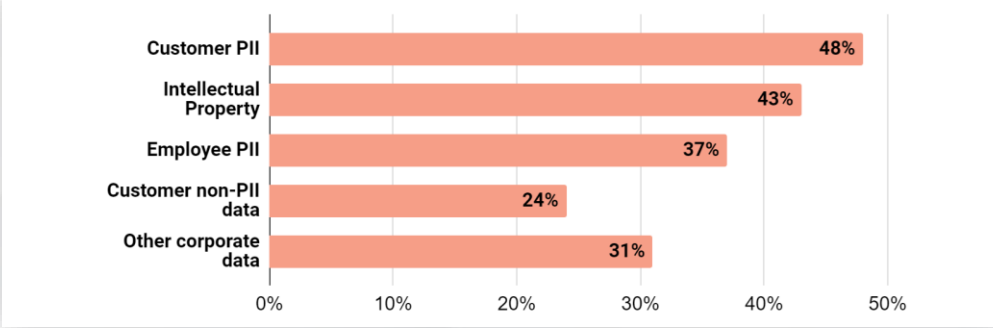

## Who discovered the cyber attack?




## Do cyber extortionists keep their promises once they've been paid?




## What type of data is targeted in cyberattacks?




Sources: Palo Alto Networks Unit 42 Incident Response Report, 2024; IBM Cost of a Data Breach Report, 2024

# Financial Impacts are large and growing

**>1,000%**

Increase in ransomware incidents since 2019

**>50%**

Increase in public extortion incidents since 2022

Largest Ransom Payment

**$40M**

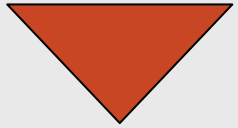
First

**>$1B**

**Impact**

From cyber incident

Tangible stock price impacts



-4%

Average share price change two weeks after initial 8-K

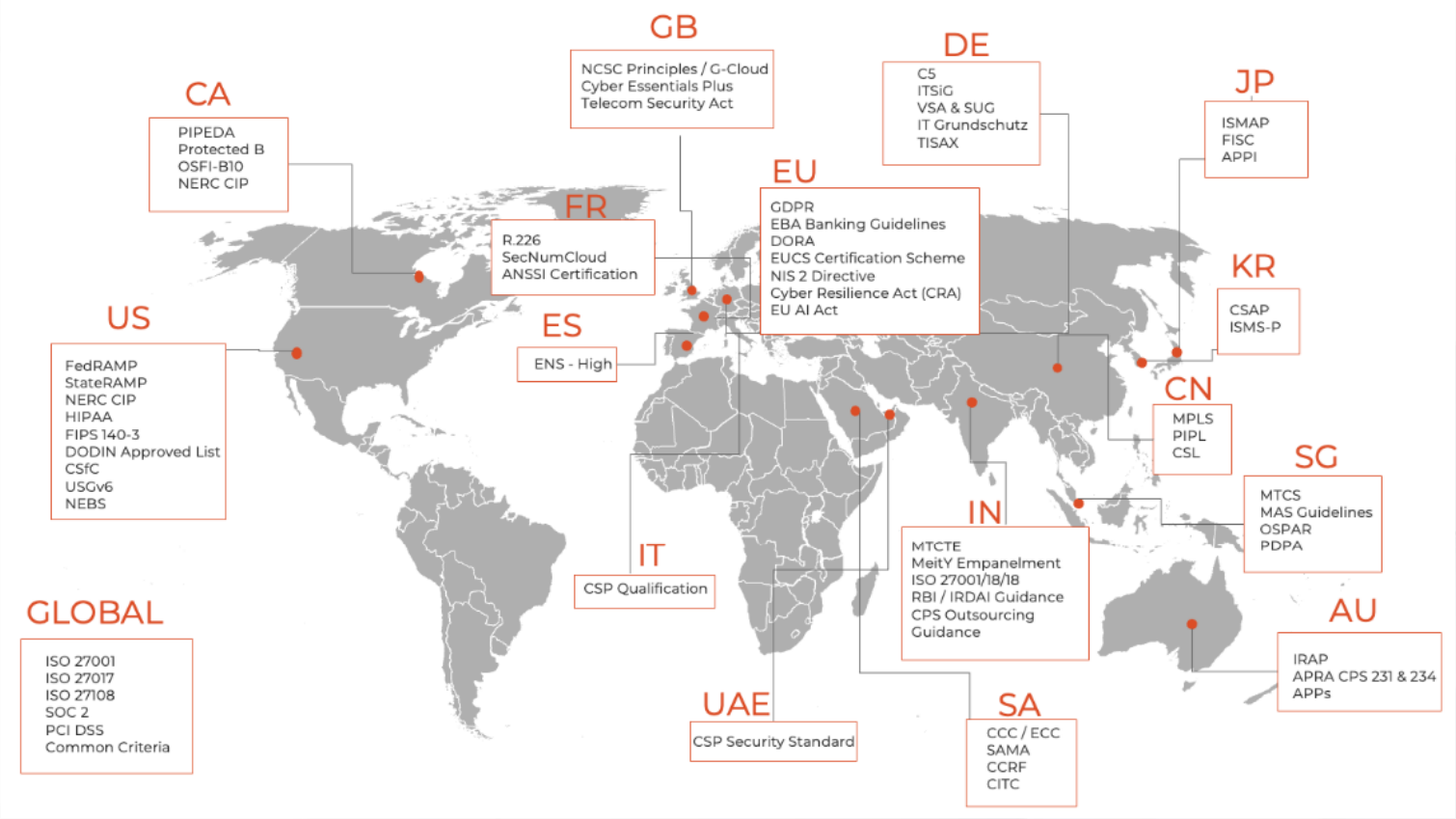
**>20%**

saw stock price decrease by more than 10%

Sources: Marsh / Guy Carpenter, Aon, Axa, NCC Group, Palo Alto Networks Unit 42, IBM

# The global cybersecurity regulatory landscape is complex



# Global regulators are also imposing stiff penalties

## Examples of implications of non-compliance with Cyber Resilience provisions

**DORA:** **1% of the average daily global turnover** of the organisation in the preceding business year. This will be applied by the Lead Overseer **daily** until compliance is achieved for no more than a period of **six months**.

**EU-NIS 2:** upto **10,000,000 Euros** or 2% annual turnover

**EU-GDPR:** Max **20,000,000 Euros** or 4% annual turnover (whichever greater)

**UK-GDPR:** Max **£17,500,000** or 4% annual turnover (whichever greater)

**SOX**: Up to **$1,000,000** or 10 years incarceration

**PCI-DSS:** **$5,000-100,000 per month** of non-compliance

**Bank Secrecy Act:** **$250,000** and 5 years incarceration

**GLBA:** **$100,000 per violation** for org, **$10,000 per violation** + 5 years incarceration for officers / directors

**PSD2:** Upto **20,000,000 Euros** or 4% annual revenue (whichever greater)

**C-11:** Upto **$10,000,000** or 3% global revenue (whichever greater)

**FFIEC:** upto **$2,000,000**

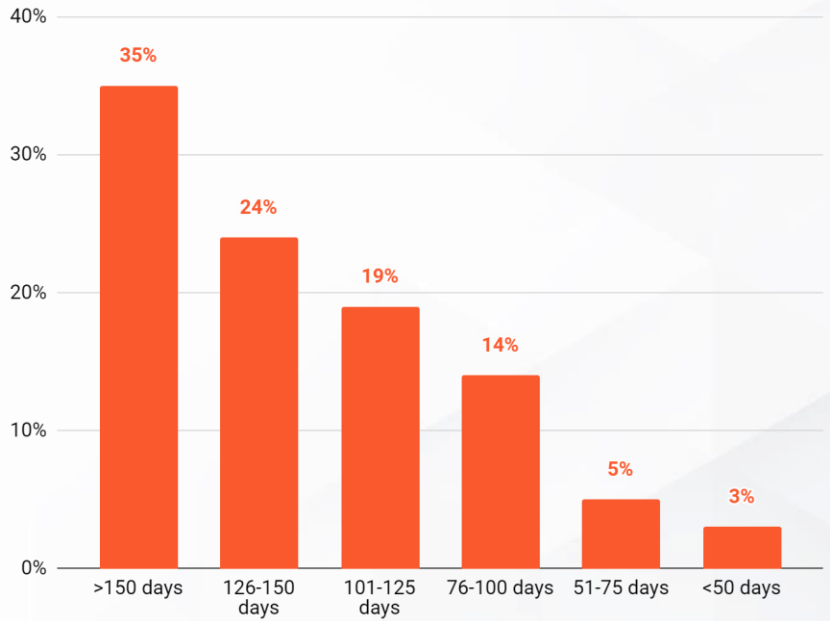
**UK Cyber Security and Resilience:** **TBD**

**PS21/3:** **TBD,** implications for digital supply chain / outages

# Three-quarters of breaches have recovery time of more than 100 days

## Average time to recover from a data breach




**70%**

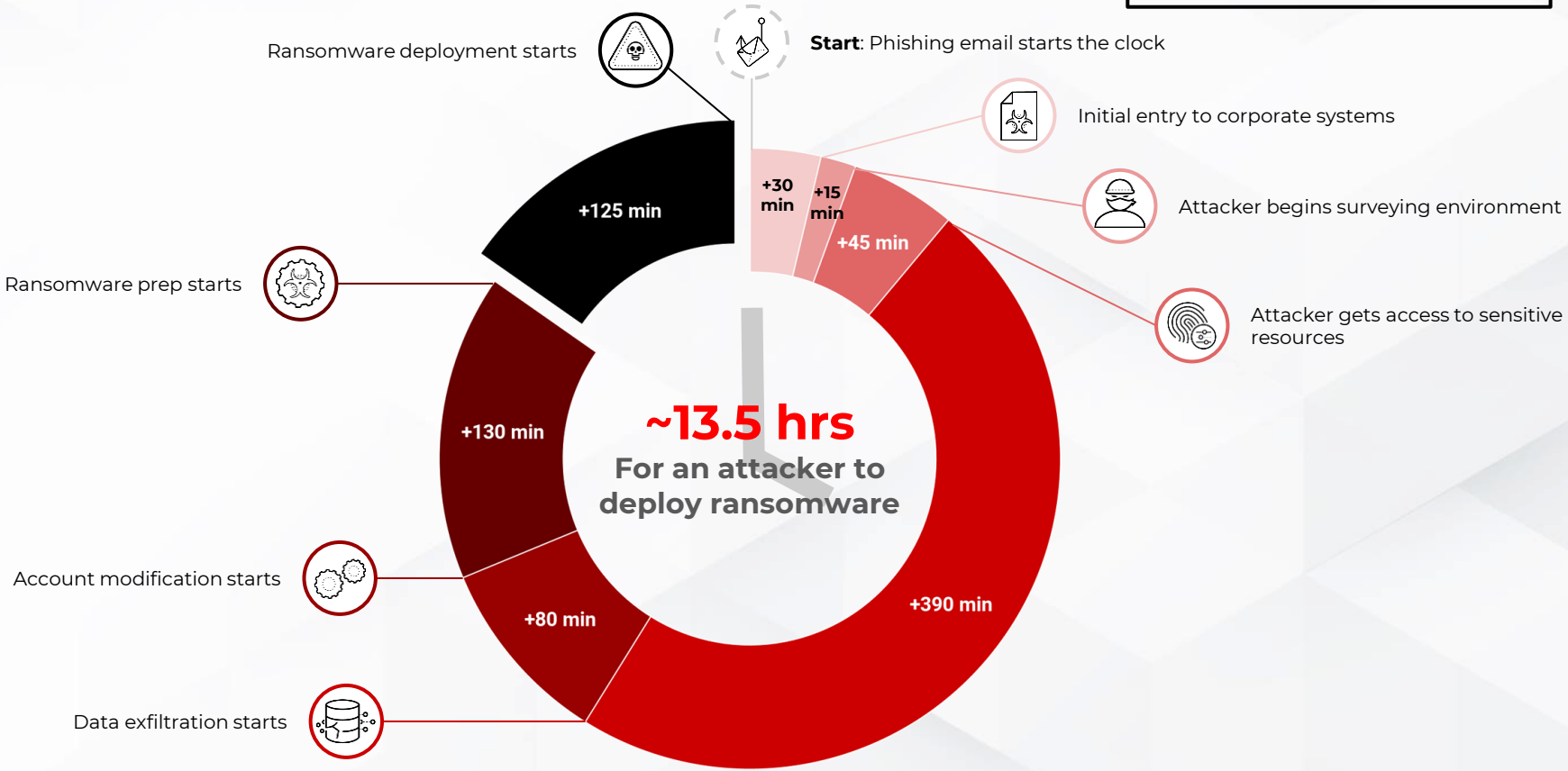
**Of breaches involved significant business disruption**

Sources: IBM, Cost of a Data Breach report

 | 

# Anatomy of a sophisticated cyber attack

**Casefile: Black Basta Ransomware**

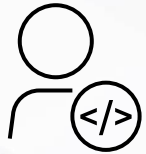


# Multiple stakeholders need to come together to mitigate cyber risk

CEO

CFO



Business Unit Head

Legal

Communications

Finance

Risk / Compliance

CIO / Head of IT

CISO

**Board of Directors Cybersecurity Committee**

# How CFOs can take responsibility for cybersecurity risk

Include cyber risk as **part of your risk oversight** and **disclose adequately**

Ensure Audit Committee and **Board level visibility** of cyber risk

Influence cyber security spending towards **risk mitigation**

Partner with internal teams for **better cyber crisis and incident preparedness**

# The trend in the cybersecurity market is towards vendor consolidation

## Crowded vendor landscape, average customer has 35+ vendors

Zoom in example:



## No incremental risk mitigation with higher cost and complexity

# >75%

**of customers are actively pursuing vendor consolidation**

**Gartner predicts:**
**By 2028, 45% of organisations will use fewer than 15 cybersecurity tools, up from 13% in 2023**

Sources: Marsh / Guy Carpenter, Aon, Axa, NCC Group, Palo Alto Networks Unit 42, IBM

# What you can do Monday morning to start mitigating cyber risk

Review **holistic cybersecurity strategy** with CISO

Understand current cybersecurity **tool estate** and **their effectiveness**

Ensure insurer **best practices** are being incorporated

Connect with leadership team to **prepare and address risks**

# Resources

2024 Unit 42 Incident Response Report

2023 Attack Surface Report

2023 Unit 42 Ransomware and Extortion Report

Unit 42 'Threat Vector' Podcast on Apple, Google, Spotify, etc.

| Unit 42 Incident Responders | | |
|---|---|---|
| **North America**<br>+1-866-486-4842<br>+1-866-4-UNIT42 | **UK**: +44-20-3743-366 | **APAC**: +65-6983-8730 |
| | **EMEA**: +31-20-299-3130 | **Japan**: +81-50-1790-0200 |