
ITC SECURE
CYBER SUMMIT
2023
ITC CYBER SUMMIT 2023
Addressing the biggest trends in cyber security
Reframe the conversation | #ITCCyberSummit
Microsoft
DARKTRACE

ITC SECURE | CYBER SUMMIT 2023

# Welcome

## Mark Weait

Chief Revenue Officer

ITC Secure

# INDUSTRY RECOGNITION

ITC SECURE | CYBER SUMMIT 2023









ITC SECURE | CYBER SUMMIT 2023

# Review of 2022


## Arno Robbertse

Chief Executive

ITC Secure

ITC SECURE | CYBER SUMMIT 2023

# The State of the Nation


## Lt. Gen. Sir Graeme Lamb
**KBE, CMG, DSO**

Chairman of the ITC Cyber Advisory Council and former Director of UK Special Forces

ITC SECURE | CYBER SUMMIT 2023

# Do More with Less


## José Lázaro Pinos

Security Solutions Expert
Microsoft

Microsoft

# Microsoft Digital Defense Report 2022

**Illuminating the threat landscape and empowering a digital defense.**

Speaker: José Lázaro Pinos

Cloud Solution Architect – Security

aka.ms/JosePinos365

# About the report:

**132** Microsoft contributors

**5** Chapters:
The State of Cybercrime
Nation State Threats
Devices and Infrastructure
Cyber Influence Operations
Cyber Resilience

**113** Pages of data, analysis, discussion, and actionable insights

## Our unique vantage point

**37bn**
email threats blocked

**34.7bn**
identity threats blocked

**43tn**
signals synthesized daily, using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

**8,500+**
engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across 77 countries.

**15,000+**
partners in our security ecosystem who increase cyber resilience for our customers.

**2.5bn**
endpoint signals analyzed daily

July 1, 2021 through June 30, 2022

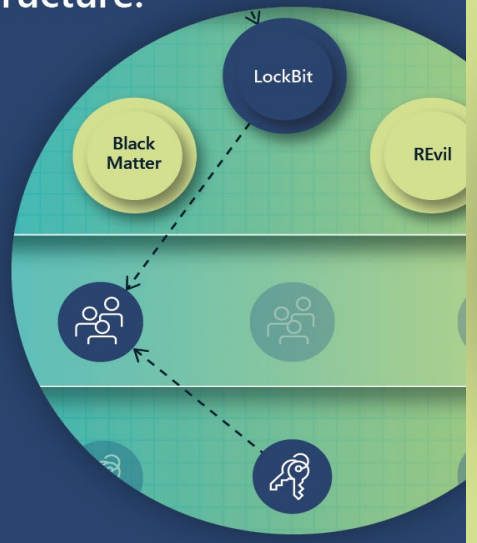
# The State of Cybercrime

As cyber defenses improve and more organizations are taking a proactive approach to prevention, attackers are adapting their techniques.

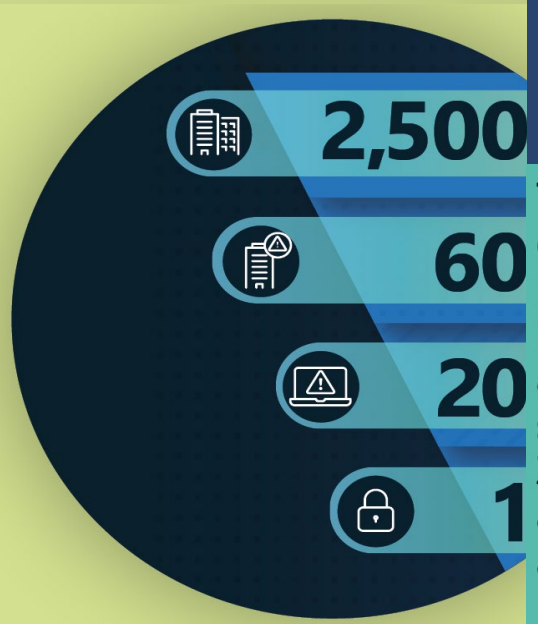
# The State of Cybercrime: Key takeaways

**Cybercrime continues to rise as the industrialization of the cybercrime economy lowers the skill barrier to entry by providing greater access to tools and infrastructure.**

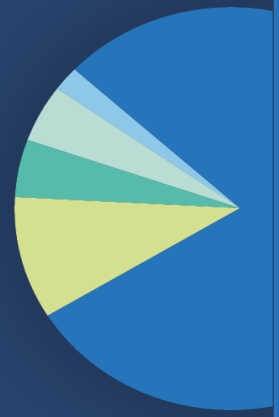
**The threat of ransomware and extortion is becoming more audacious with attacks targeting governments, businesses, and critical infrastructure.**



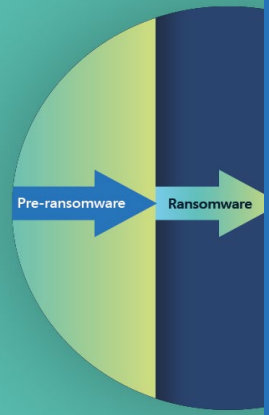

Human operated ransomware is most prevalent, as one-third of targets are successfully compromised by criminals using these attacks and 5% of those are ransomed.



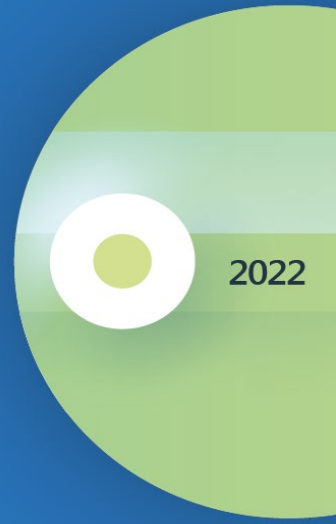

**Credential phishing schemes which indiscriminately target all inboxes are on the rise and business email compromise, including invoice fraud, poses a significant cybercrime risk for enterprises.**



**The most effective defense against ransomware includes multifactor authentication, frequent security patches, and Zero Trust principles across network architecture.**




To disrupt the malicious infrastructures of cybercriminals and nation state actors, Microsoft relies on innovative legal approaches and our public and private partnerships.



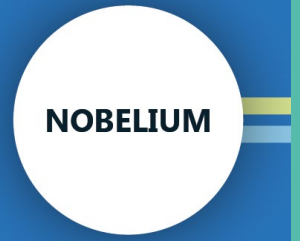
# Nation State Threats

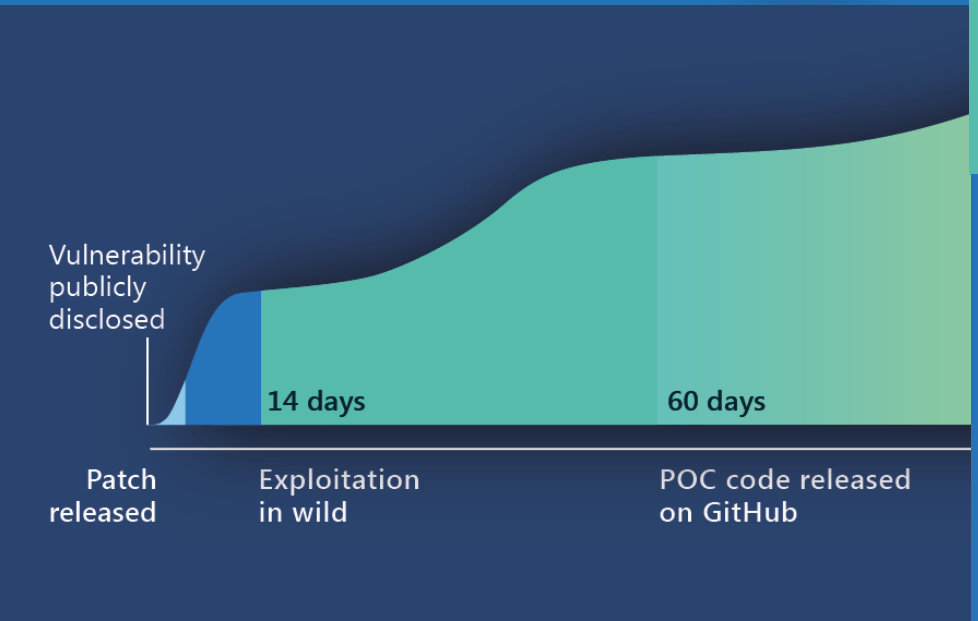
Nation state actors are launching increasingly sophisticated cyberattacks to evade detection and further their strategic priorities.

# Nation State Threats: Key takeaways

Increased targeting of critical infrastructure particularly IT sector, financial services, transportation systems, and communications infrastructure.

IT supply chain being used as a gateway to access targets.




China expanding global targeting especially smaller nations in Southeast Asia, to gain intelligence and competitive advantage.

Iran grew increasingly aggressive following power transition, expanded ransomware attacks beyond regional adversaries to US and EU victims, and targeted high profile US critical infrastructure.

North Korea targeted defense and aerospace companies, cryptocurrency, news outlets, defectors, and aid organizations, to achieve regime's goals: to build defense, bolster the economy, and ensure domestic stability.

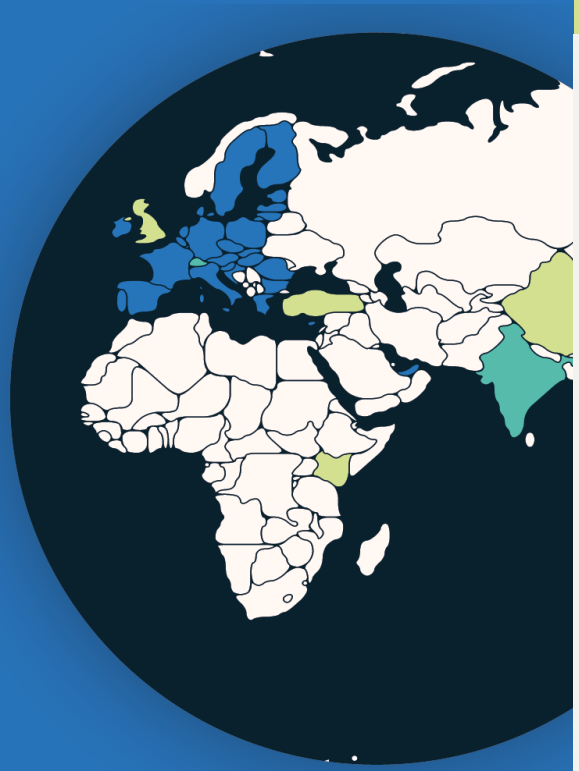
Cyber mercenaries threaten the stability of cyberspace as this growing industry of private companies is developing and selling advanced tools, techniques, and services to enable their clients (often governments) to break into networks and devices.

# Devices and Infrastructure

With the acceleration of digital transformation, the security of digital infrastructure is more important than ever.

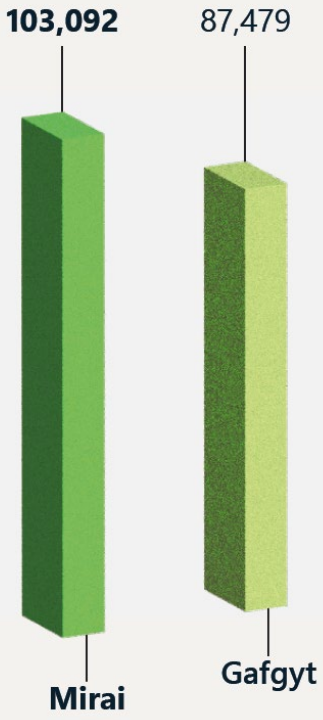
# Devices and Infrastructure: Key takeaways

Governments worldwide are moving to protect critical infrastructure by improving IoT and OT security.



Globally consistent and interoperable security policies are needed to ensure broad adoption.

Malware as a service has moved into large scale operations against exposed IoT and OT in infrastructure and utilities as well as corporate networks.




Attackers are increasingly leveraging vulnerabilities in IoT device firmware to infiltrate corporate networks and launch devastating attacks.

Attacks against remote management devices are on the rise, with more than 100 million attacks observed in May of 2022—a five-fold increase in the past year.

32% of firmware images analyzed contained at least 10 known critical vulnerabilities.

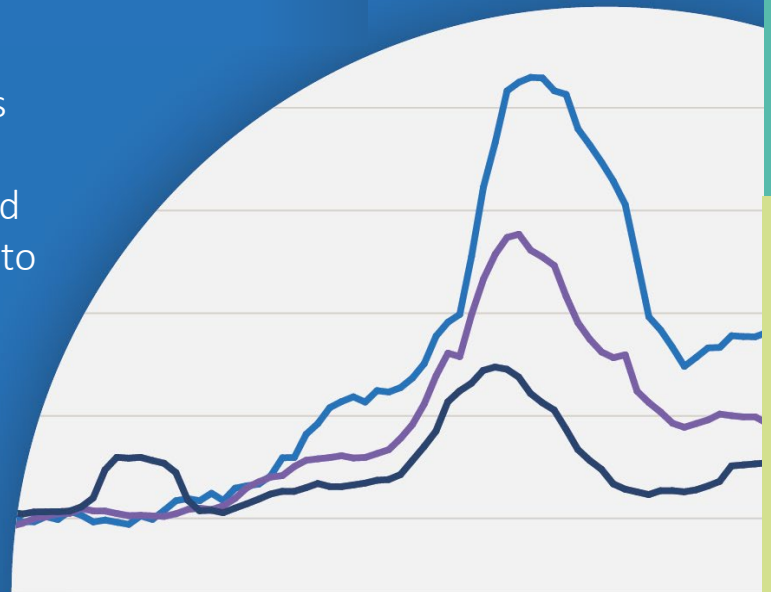
# Cyber Influence Operations

Today's foreign influence operations utilize new methods and technologies, making their campaigns designed to erode trust more efficient and effective.

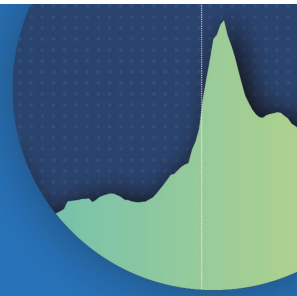
# Cyber Influence Operations: Key takeaways

Cyber influence operations are becoming increasingly sophisticated as more governments and nation states are using these operations to shape opinion, discredit adversaries, and promote discord.

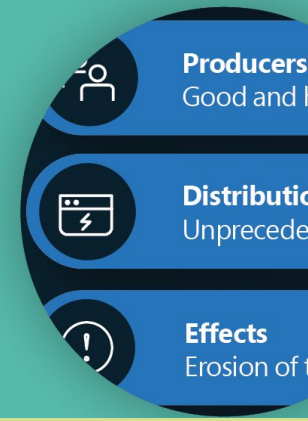

Cyber influence operations integrated with more traditional cyberattacks and kinetic military operations to maximize impact.



Russia, Iran, and China employed propaganda and influence campaigns throughout the COVID-19 pandemic often as a strategic device to achieve broader political objectives.



Synthetic media is becoming more prevalent due to the proliferation of tools which easily create and disseminate highly realistic artificial images, videos, and audio. Digital provenance technology that certifies media asset origin holds promise to combat misuse.




## A holistic approach to protect against cyber influence operations

Microsoft is building on its already mature cyber threat intelligence infrastructure to combat cyber influence operations. Our strategy is to detect, disrupt, defend, and deter propaganda campaigns by foreign aggressors.

# Cyber Resilience

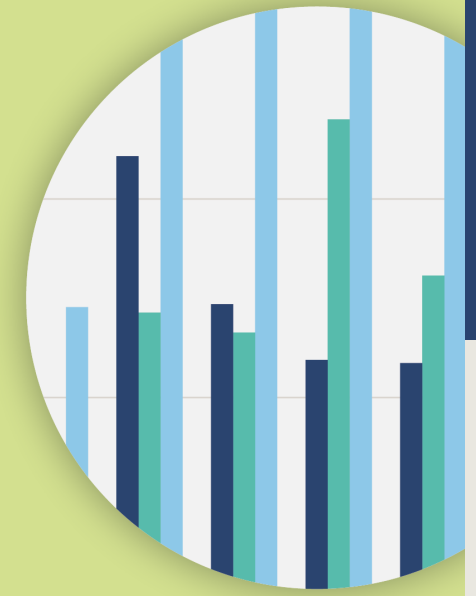
Understanding the risks and rewards of modernization becomes crucial to a holistic approach to resilience.

# Cyber Resilience: Key takeaways

Effective cyber resiliency requires a holistic, adaptive approach to withstand evolving threats to core services and infrastructure.

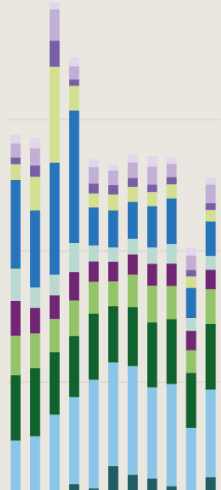
Modernized systems and architecture are important for managing threats in a hyperconnected world.

While password-based attacks remain the main source of identity compromise, other types of attacks are emerging.



The vast majority of successful cyberattacks could be prevented by using basic security hygiene.

Over the past year, the world experienced DDoS activity that was unprecedented in volume, complexity, and frequency.

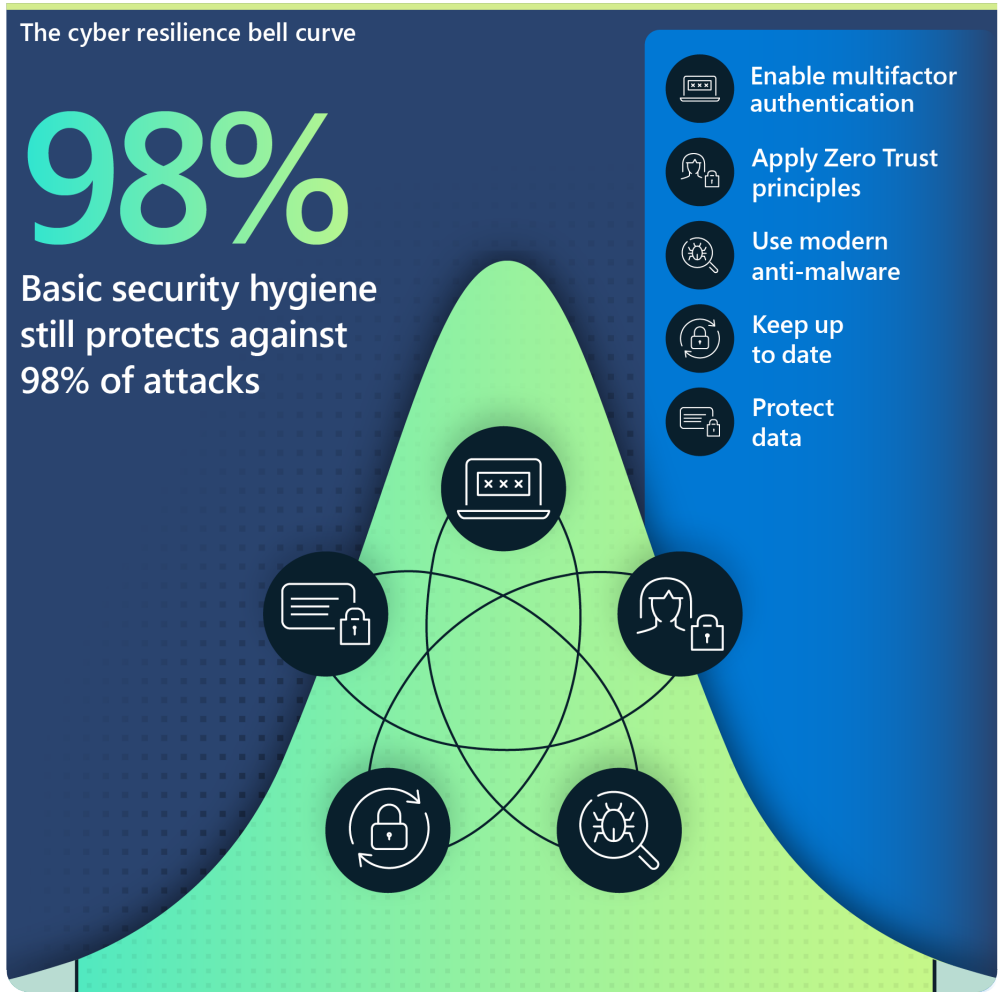


Basic security posture is a determining factor in advanced solution effectiveness.

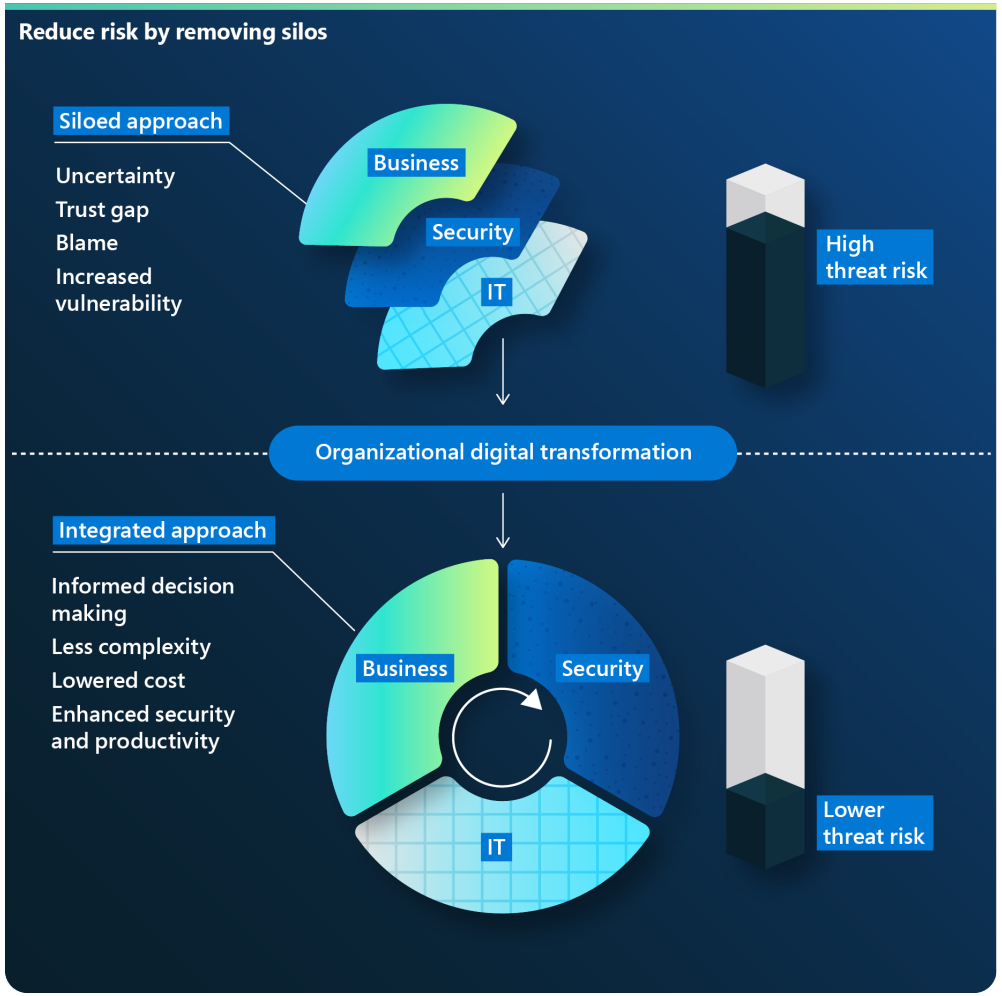
The human dimension of resilience to cyber influence operations is our ability to collaborate and cooperate.

# Cyber Resilience continued

## Resilience success factors every organization should adopt




## Integrate business, security, and IT for greater resilience



Microsoft Security

# Do More with Less

# CISOs are under pressure to contain costs

Conventional security tools **have not kept pace**

Cost of security breaches **is rising**

Resources are **constrained**

***"Boards are now pushing back for improved understanding of what they have achieved after years of such heavy investment."*** [1]

Gartner

Paul Proctor
Distinguished VP Analyst, Gartner

Significantly more security decision makers have felt pressure to cut costs within the past 6 months[2]

**82%**

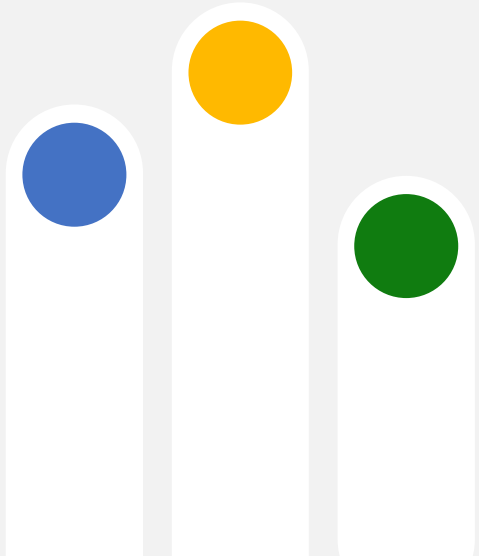
feel pressured to lower costs[3]

**#1**

priority to reduce cost is improved threat protection

[1] "The Urgency to Treat Cybersecurity as a Business Decision" February, 2020
[2] March 2022 survey of 501 US Security Decision Makers commissioned by Microsoft from agency, Vital Findings
[3] "Microsoft Pandemic CISO Survey" 2020

Microsoft Security helps you do more with less



## Simplify Vendor Management

## Reduce Threats with AI and Automation

## Improve Operational Efficiency

# Simplify vendor management


Replace up to

**50**

product categories

Up to

**60%**

savings with Microsoft 365 E5 Security and Microsoft 365 E5 Compliance[1]

**$0**

built in Cloud Security Posture Management with Microsoft Defender for Cloud

**30%**

average savings from unifying cloud security tools with Microsoft Defender for Cloud[2] for organizations in a Microsoft commissioned study

[1] Savings based on publicly available estimated pricing for other vendor solutions and Web Direct/Base Price shown for Microsoft offerings

[2] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Azure Security Center," June, 2021, commissioned by Microsoft

# Getting up to 60% savings

## $63 per user

**Compliance ($33)**

Compliance Management
Search and eDiscovery; Auditing (Advanced)
Insider Risk Management; Access Control
Information Protection and Governance

**Security ($30)**

Identity and Access Management
Intrusion detection, investigation, prevention, and threat intelligence
Email protection
Endpoint Protection and Response
Cloud Access Security Broker

**Examples of multi-vendor standalones**

← **$39 more** per user

## $24 per user

Microsoft 365 E5 Compliance add-on to Microsoft 365 E3 — ($12)

Microsoft 365 E5 Security add-on to Microsoft 365 E3 — ($12)

**Full E3 suite**

Microsoft 365

**Up to 60% savings**

Web Direct/Base Price shown for Microsoft offerings. Multi-vendor prices based on publicly available estimated pricing for other vendor solutions and are illustrative.

# Reduce threats with AI and Automation


**60%**

reduced risk of material breach[1]

**65%**

Less time to investigate threats[1]

**88%**

less time responding to threats with Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud[1]

**$10.5**

million additional end user productivity from automation and process improvements in Microsoft 365 Defender[2]

In Microsoft commissioned studies from **Forrester Consulting,** organizations averaged significant savings:

**96%**

less time spent monitoring potential suspicious activity with Microsoft Purview[3]

**90%**

reduced alert fatigue, elevating the most critical issues with Microsoft Sentinel[4]

[1] Forrester Consulting, "The Total Economic Impact™ Of Microsoft SIEM and XDR", August 2022, commissioned by Microsoft
[2] Forrester Consulting, "The Total Economic Impact™ Of Microsoft 365 Defender", April 2022, commissioned by Microsoft
[3] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft 365 E5 Compliance," June, 2021, commissioned by Microsoft
[4] Microsoft blog: Azure Sentinel uncovers the real threats hidden in billions of low fidelity signals, Feb 2020

# Cost savings | AI and Automation

In Microsoft commissioned studies from Forrester Consulting, organizations averaged significant savings

## Reduce Total Cost of Risk

| | |
|---|---|
| **Microsoft Security solutions** | Enhanced security reduced the risk of a data breach by 50%[1] |
| **Microsoft Purview** | Reduced costs from data breaches by 40-50%[2] |
| **Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud** | Reduced risk of material breach by 60%<br>Reduced time to investigate threats by 65%<br>Reduced time to respond to threats by 88%[3] |
| **Azure Active Directory** | Reducing the complexity of IAM solutions reduced risk of a security breach by 45%[4] |

## Save On Automation and Process Improvements

| | |
|---|---|
| **Microsoft Sentinel** | Reduced false positives 79%[5]<br>Reduced alert fatigue by 90%, elevating the most critical issues[6] |
| **Azure Network Security** | Automated upgrades and improved visibility reduced risk of a security breach of 30%[7] |
| **Microsoft 365 Defender** | Increased end user productivity from automation and process improvements valued at $10.5 million[8] |
| **Microsoft Cloud App Security** | Automated processes eliminated 75% of threats automatically[9] |
| **Microsoft Security solutions** | Reduced resources required for audit and compliance management by 25%[1] |

[1] Forrester Consulting, "The Total Economic Impact™ Of Zero Trust Solutions From Microsoft", December 2021, commissioned by Microsoft
[2] Forrester Consulting, "The Total Economic Impact Of Microsoft 365 E5 Compliance," February, 2021, commissioned by Microsoft
[3] Forrester Consulting, "The Total Economic Impact™ Of Microsoft SIEM and XDR", August 2022, commissioned by Microsoft
[4] Forrester Consulting, "The Total Economic Impact Of Microsoft Azure Active Directory," August, 2020, commissioned by Microsoft
[5] Forrester Consulting, "The Total Economic Impact Of Microsoft Azure Sentinel," November, 2020, commissioned by Microsoft
[6] Microsoft blog: Azure Sentinel uncovers the real threats hidden in billions of low fidelity signals, Feb 2020
[7] Forrester Consulting, "The Total Economic Impact Of Microsoft Azure Network Security" May, 2021, commissioned by Microsoft
[8] Forrester Consulting, "THE TOTAL ECONOMIC IMPACT™ OF MICROSOFT 365 DEFENDER", April 2022, commissioned by Microsoft
[9] Forrester Consulting, "The Total Economic Impact™ Of Microsoft Cloud App Security", May 2020, commissioned by Microsoft

*"The **automation and orchestration** inherent in the Microsoft 365 platform combined with the **security of the tools** was a **differentiator** for us."*

**Lawrence Zorio**
Vice President IT Information, Smith+Nephew

# Improve Operational Efficiency


In Microsoft commissioned studies from **Forrester Consulting,** organizations averaged significant savings

**67%**

**reduced time to deployment with Microsoft Sentinel[1]**

**73%**

**improved efficiency of network-related IT work with Azure Network Security[2]**

**75%**

**reduction in password requests after introducing**

**Self-service Single-Sign-On (SSO) with Azure Active Directory[3]**

**$479k**

**in human capital freed up by redeploying IT time with Microsoft Endpoint Manager[4]**

[1] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Azure Sentinel," November, 2020, commissioned by Microsoft
[2] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Azure Network Security" May, 2021, commissioned by Microsoft
[3] Forrester Consulting, "The Total Economic Impact™ Of Zero Trust Solutions From Microsoft", December 2021, commissioned by Microsoft
[4] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Endpoint Manager," April 2021, commissioned by Microsoft

# Cost savings | Improved Operational Efficiency

In Microsoft commissioned studies from Forrester Consulting, organizations averaged significant savings

## IT Admin and Deployment Savings

| | |
|---|---|
| **Microsoft Endpoint Manager** | Reduced support needs saved the organization **$1.5 million**<br>Redeployed IT time **frees up $479,000 in human capital**, to be applied to under-resourced projects[1] |
| **Microsoft Security solutions** | Reduced the effort required to provision and secure new infrastructure by **80%**[2] |
| **Microsoft Sentinel, Microsoft 365 Defender,** and **Microsoft Defender for Cloud** | Reduced time to create a new workbook by **90%**<br>Reduced time to onboard new security professionals by **91%**<br>Improved productivity of other employees by almost **68,000 hours** annually[3] |
| **Azure Active Directory** | Self-service Single-Sign-On (SSO) reduced password reset requests by **75%,** saving $2.9 million/year and users **10 minutes per week**[4] |
| **Azure Network Security** | Improved efficiency of network-related IT work by **73%**<br>Reduced the number of security and IAM-related help desk calls by **50%**<br>Accelerated the process to set up end users on new devices by **75%**[5] |
| **Microsoft Purview** | Decreased the time spent on ongoing monitoring and checking indicators of potential suspicious activity by **96%**<br>Improved process efficiency valued at **$3.1 million**[6] |
| **Microsoft Defender ATP** | Reduced SecOps and IT efforts for efficiency gains of **$601,792**<br>Recovered business end user productivity valued at **$3,135,789**[7] |
| **Microsoft 365 Defender** | Increased the efficiency of security teams by **50%**[2] |
| **Microsoft Cloud App Security** | Reduced time and effort to remediate incidents by **80%**[8] |

[1] Forrester Consulting, "The Total Economic Impact™ Of Microsoft Endpoint Manager," April 2021, commissioned by Microsoft
[2] Forrester Consulting, "The Total Economic Impact™ Of Zero Trust Solutions From Microsoft", December 2021, commissioned by Microsoft
[3] Forrester Consulting, "The Total Economic Impact™ Of Microsoft SIEM and XDR", August 2022, commissioned by Microsoft
[4] Forrester Consulting, "The Total Economic Impact™ Of Microsoft Azure Active Directory," August, 2020, commissioned by Microsoft
[5] Forrester Consulting, "The Total Economic Impact™ Of Microsoft Azure Network Security" May, 2021, commissioned by Microsoft
[6] Forrester Consulting, "The Total Economic Impact™ Of Microsoft 365 E5 Compliance," February, 2021, commissioned by Microsoft
[7] Forrester Consulting, "The Total Economic Impact™ Of Microsoft Defender ATP", April 2019, commissioned by Microsoft
[8] Forrester Consulting, "The Total Economic Impact™ Of Microsoft Cloud App Security", May 2020, commissioned by Microsoft

*"It's about making **the right** security investments, not necessarily investing more. Making sure all of your systems work together so that threats are caught early and remediation can be swift."*

**Bret Arsenault**
VP and CISO,
Microsoft

Microsoft Security

# Thank you.

# Networking Break

ITC SECURE | CYBER SUMMIT 2023

ITC SECURE | CYBER SUMMIT 2023

# Exclusive Keynote

## Dave Cartwright

Head of Technology Operations & Risk
/ Chief Information Security Officer
Santander International

ITC SECURE | Santander International

# What we'll have to defend against in 2023

## And what we can do, apart from throwing money at it

Microsoft DARKTRACE

# Who am I?

CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

bcs Fellow

(ISC)²

CISSP®

The Register®

Chartered Institute of Information Security

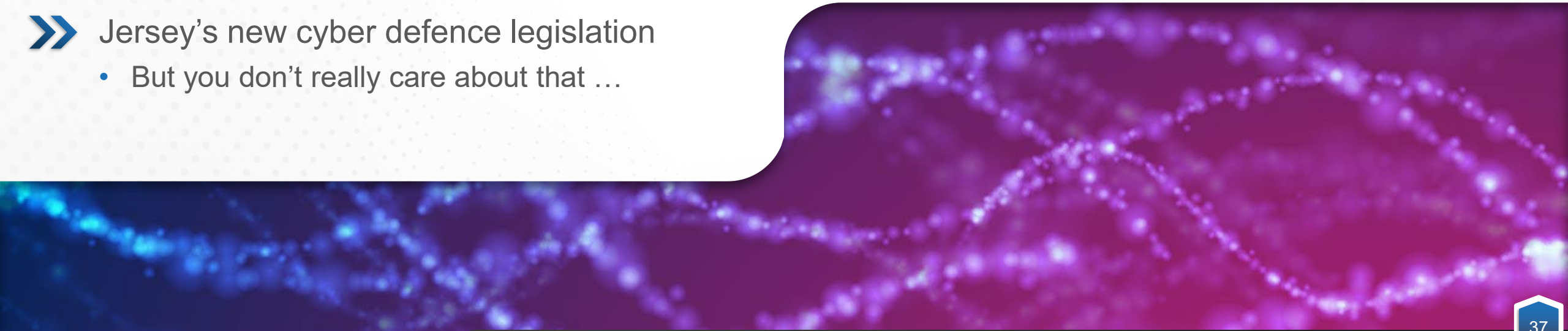
# What I’m expecting in 2023

# The top five threats right now

- My favourite threat analyst sees these as his top five:
  - Ransomware
  - Supply chain/third-party risk
  - Insider threat
  - Data breach
  - Wiper and other destructive malware
- These will continue in pretty much this order through 2023
- But we do need to think of the context/jurisdiction
  - For instance, insider threat is much less common in the Channel Islands than in larger countries

# What else will be big in 2023?

- Cyber insurance – for all the wrong reasons
  - Premiums are going up, breadth of coverage is going down
- New types of tech will hit the market, so attacks will be developed for them
  - Particularly car technology
- Jersey's new cyber defence legislation
  - But you don't really care about that …
- AI tools like ChatGPT will grow exponentially
  - And they'll be pretty poor and will introduce security problems
- Biometric security, popular in personal tech, will grow in the enterprise
  - Though we need to remember the drawbacks



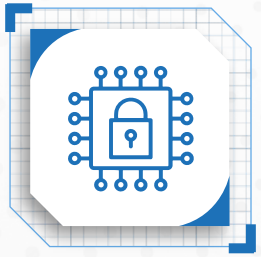
# There are loads of commercial solutions out there

SOAR platforms

- (Security Orchestration, Automation and Response)

SIEM systems

- (Security Information and Event Management)



IDS/IPS tools for the edge of the network

- (Intrusion Detection / Prevention System)

EDR solutions

- (Endpoint Detection and Response)

Vulnerability scanners

IBM

splunk>

cybereason

Microsoft

Qualys.

CISCO

CROWDSTRIKE

DARKTRACE

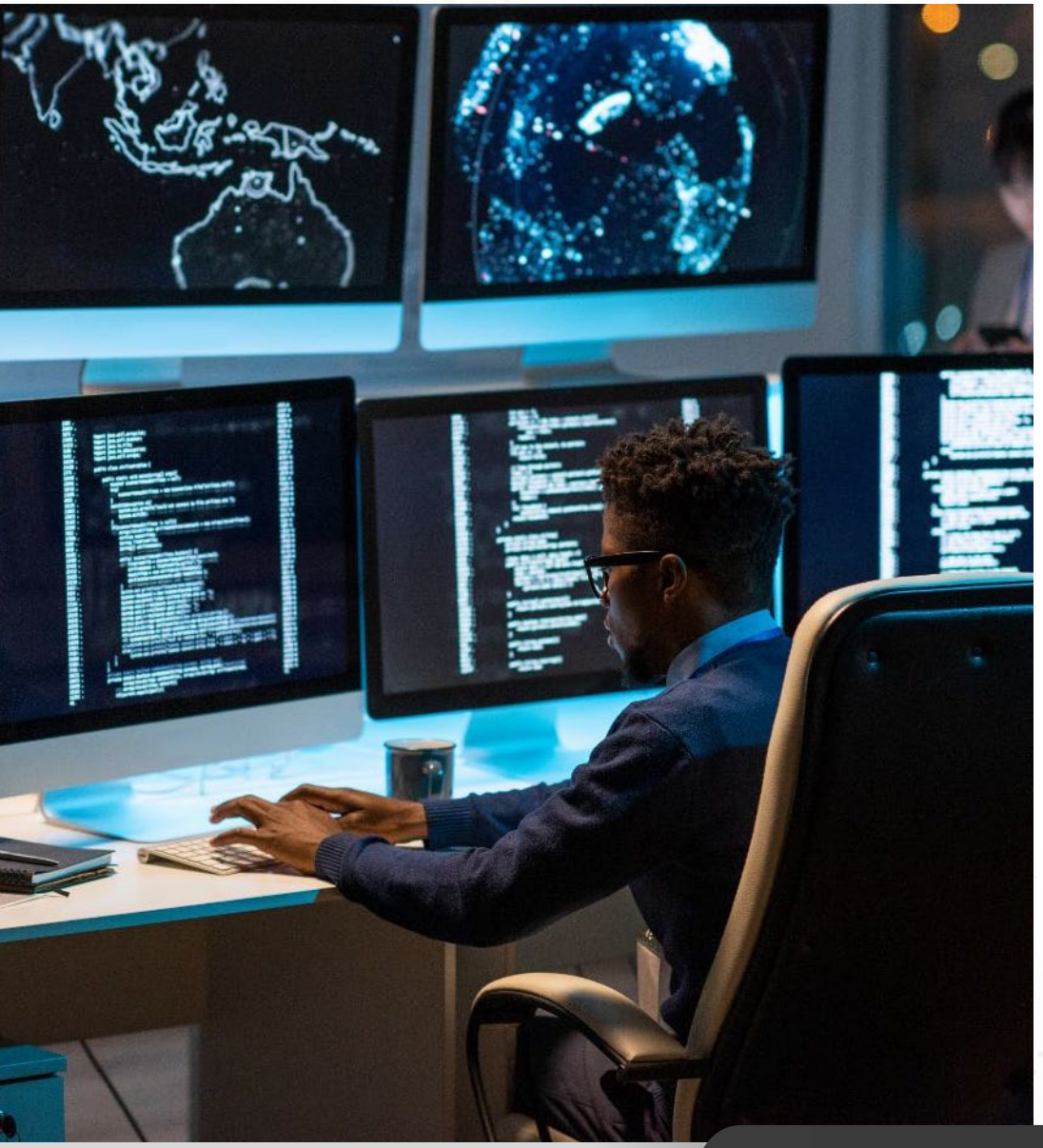
# But there's an elephant in the room

- We generally don't get value from the (expensive) security tools we buy
  - Who has FPF – False Positive Fatigue – from the SOAR system?
  - What proportion of SIEM alerts are acted upon?
  - Is the enterprise anti-malware installed on 100.0% of all devices?
    - Exceptions, in this sense, are the enemy of the CISO
- In fact, we hardly use the ones we get for free!
  - Who genuinely has a schedule of looking at Windows security logs?
  - Who has a regimented review programme for checking firewall rejections?
  - Do we do regular reviews of Office 365 security with the tools O365 gives us?
- And sometimes we don't even understand the free stuff properly
  - Who understands what the ROBOTS.TXT file on your web server does?

# “Take a risk-based approach”

- When I’m asked where you start with cyber security:
  “It’s an instance of business risk”
- So-called security standards like ISO 27001 start with a risk assessment
  - Well, they do just after the bit about “top management buy-in”
- But let’s be a little bit pragmatic here
- If we’re building an office, we’ll include fire escapes and probably an intruder alarm
- Even if it’s not a legal requirement, some stuff is just obvious
  - And that’s because every risk assessment ever has identified it
  - So why do we need to jump through hoops to get the answer we already know?
- “If you wish to make an apple pie from scratch, you must first invent the universe”

# Start with the stuff you just need to do



- There are some obvious things to do in cyber that are such no-brainers you don't need a risk assessment
  - Anti-malware software on every system
  - Change all the default passwords, and disable generic admin accounts if you can
    - And generally control who has access to what
- Have a NAT firewall between you and the internet
- Keep your systems patched up to date
  - And replace obsolete kit
- Use the most secure settings you can
  - MFA is your best friend
- These are all cheap and easy – so just do them, and do them properly
  - And don't write any of them off as "too hard"

# What about awareness training?

- I could do an hour on awareness training in its own right
  - But not here
- There's no excuse for not doing it
  - There are many inexpensive commercial awareness programmes
  - And if you have a user-induced breach, the ICO will ask some searching questions
- A brief precis, then:
  - Make it regular
  - Make it as non-dull as you can
  - Try to use different media (talks, online stuff, simulations)
  - Target it at all levels – senior management are different from junior staff

# Next, look at your IFAs


- Nothing to do with financial advice – they're Internet-Facing Assets to us
- Three core areas:
  - Anything sitting facing the internet and accepting inbound connections
    - Web servers are the usual suspects
    - And maybe on-prem email servers if you're still in the Dark Ages
  - Inbound email streams
  - Web filtering and content analysis
- Anything that can bring stuff from the internet into our private network
  - Whether it's originated externally (e.g. a web server) …
  - … or internally (e.g. someone checking their O365 email in Outlook)

# Next, look at your IFAs

- If you have internet-facing kit, use a two-layer firewall
  - LAN-DMZ firewall plus DMZ-internet firewall
  - Never have the ability to route inbound directly from the internet to the LAN
    - Can only afford virtual firewalls on a single set of hardware? It'll do for now
- For web browsing control, adopt a web filtering service
  - Cloud-based ones are good value and dead easy to set up
    - Usually include filtering, malware detection and DDoS
- For inbound email, use a similar service to check for malware, impersonation, etc.
  - Catch it before it gets to the mail server if you can – PC AV can catch the stragglers
- Always use a Web Application Firewall on your website
  - Cloud-based WAFs are cheap and will catch most attacks in their setup, not yours
  - And maybe even use a bot blocker to enforce ROBOTS.TXT

# Then look at what an attack could do if it got in

- Many in the industry call this principle “assume breach”
- The chance of fending off 100% of attacks is negligible
  - So you need to consider how to mitigate the non-zero number that get through
- “Zero Trust”?
  - A nice idea but Zero Trust is a pain to manage, introduces MFA fatigue, and so on
- Think instead of “limited trust”
  - Ransomware example - ~50,000 of several million docs encrypted
  - Think of what I said about insurance coverage reducing
- Setting and periodically verifying permissions on file shares is tedious but inexpensive

# Vulnerability scanning

- There are three broad categories of vulnerability:
  - Those induced by lack of effective patching/upgrades
  - Those induced by misconfiguration
  - Those induced by bugs in systems
- There is no excuse for getting hacked through a hole you could have patched
  - Hit by a “Zero Day”? I feel for you, as sometimes it’s just one of those things
- Misconfiguration or bugs can be discovered with tools that probe your system
  - Try something like ImmuniWeb – cost-free for a basic scan but informative
  - If you can’t afford to do internal systems and IFAs, at least do IFAs
- If your scan shows up a vulnerability that’s fixed by a known patch, that’s bad
  - And for those fixed by configuration changes, think WannaCry

# And finally …

- With all of the above, there's a super-critical thing you need to make them any good
- You need **visibility** of what's right and what's wrong
  - Particularly what's wrong
- Every tool and action I've mentioned is inexpensive to implement and use
- But there's no point having them unless you use them properly
- And you can't use them properly unless you can see what they tell you

# My favourite example of security visibility

- Annual reviews of access to core systems (about 25-30)
- Previously hideously manual
- Could use an IAM tool like SailPoint, but these are complex and expensive
- Instead used tools they had already:
  - PowerShell (already on the servers)
  - SQL Server (large existing install base, no problem to add one database)
  - Power BI
- In three months, reduced manual effort by ~80-90%
  - A handful of apps needed hands-on actions to extract the user lists

# So what about SIEM, SOAR and the like?

- Yes, you should absolutely consider implementing them
- But only if you'll get value from them
  - You can shoot yourself in the foot by using expensive tools badly
  - Explain to the ICO how that data breach happened despite all the tools!
- Remember that to get value from tools, you need to have people to work with them
  - Many tools are under-used because of a lack of people to react to what they say
- Remember that as your security profile improves, it gets harder to improve further
  - Cyber Essentials is easy and is reckoned to help avoid ~80% of attacks
  - Getting from 80% to 90% is an order of magnitude harder
  - Getting from 90% to 95% is even harder still – and more expensive
  - The payoff of the cost gets smaller as you improve your posture

# Wrapping up

# In summary, then ...

- Sorting out the basics defends you against the majority of attacks, cheaply
- Some fairly simple actions and systems allow you to:
  - Limit the blast radius of ransomware by restricting directory access
  - Nail the vast majority of malware using off-the-shelf AV solutions
  - Separate the LAN from the internet using firewalls which cost, but not too much
  - Keep rogue traffic off your web server by letting the cloud WAF bat it off
  - Use off-the-shelf tools, which you may already have, to inform you of issues
- And once you've done that, re-assess your security risks
- Then any gap you find is where you can think of starting to spend money

# Homework

- These don't necessarily relate directly to this talk
  - But I think they're super-useful and well worth a look
- Ken Munro's **talk on hacking his kettle** at the Jersey Cyber Forum 2022
- FC's video **"How I Used to Rob Banks"**
- Matthew Syed: **"Black Box Thinking"**
- Matt Parker: **"Humble Pi"**

# Feel free to stay in touch

https://www.linkedin.com/in/davidscartwright/

@DaveTheCISO

David.Cartwright@santanderinternational.co.uk
dsc@korana.com

# THANK YOU

ITC SECURE | Santander International

# Ask the Experts


CYBER SUMMIT
2023

# Closing Remarks

ITC SECURE | CYBER SUMMIT 2023

# INDUSTRY RECOGNITION

ITC SECURE | CYBER SUMMIT 2023









# Networking Drinks

ITC SECURE | CYBER SUMMIT 2023