Columbus

Avoid the knockout

Turn security plans into action with proactive risk management

Albert Altman, Columbus

Stand up if you've used the same password for more than three sites – and one of them was Netflix.

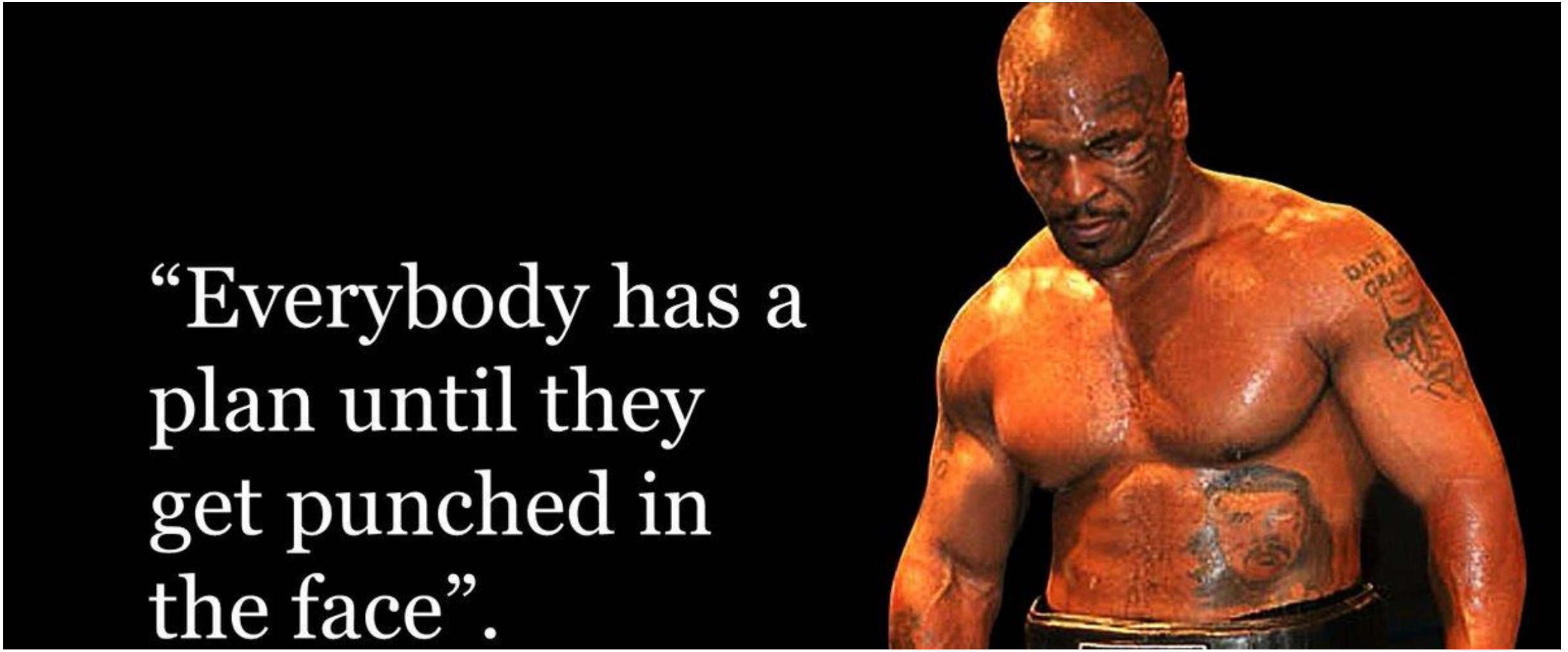
Stay standing if you've ever... clicked "Remind me later" on an update – for like a year.

Please sit down

By show of hands, how many here have a documented cybersecurity plan in their organization?

By show of hands,
How many feel that the plan is actually followed when it really matters?

By show of hands,
How many of you have conducted an incident drill or a tabletop simulation?



Michael Gerard Tyson

Never Stand Still!

In boxing, the one who stands still gets knocked out.

Same goes for cybersecurity – those who wait to act will sooner or later get hit by (among other things) malicious code.

Cybersecurity isn't a sprint – it's a martial art. And it's won with focus, training, and yes: discipline.

Technology as a line of defense is no longer enough!

Discipline is required.

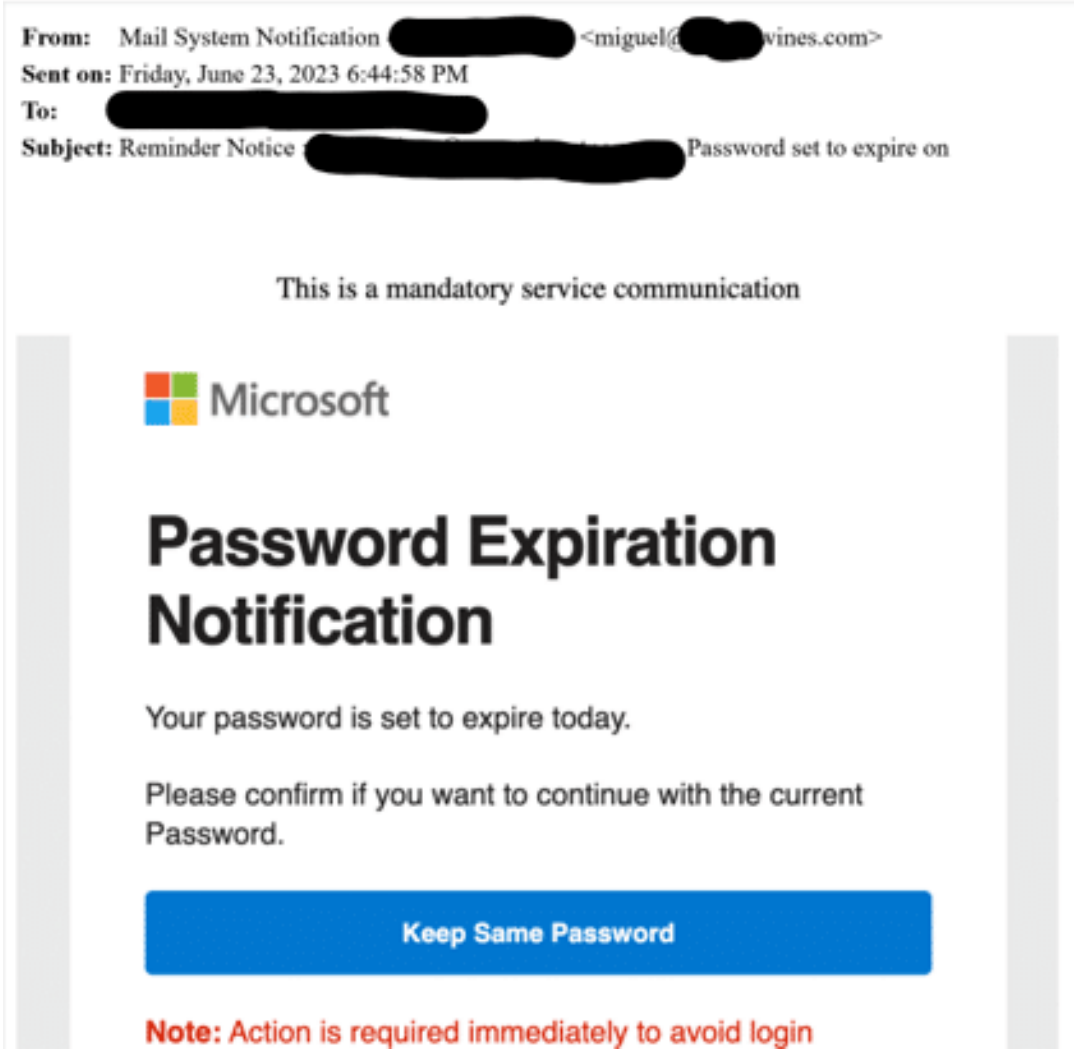
Discipline to follow **routines**, **act proactively**, and **never let your guard down**.

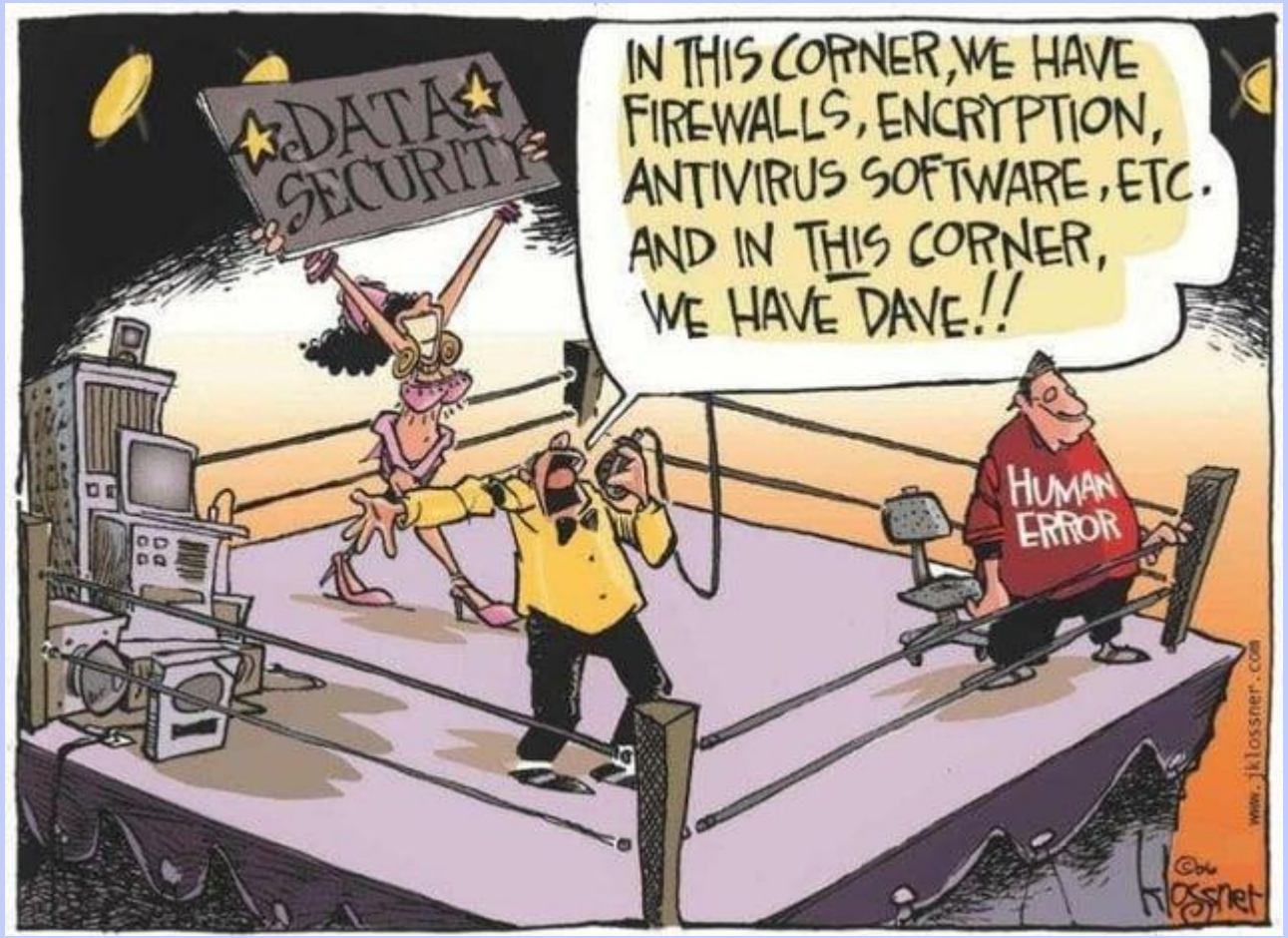
Because the question is no longer if we'll be attacked – but when, and how well-prepared we are to dodge and strike back.

You must identify weaknesses where you're most vulnerable and manage them, or the bad guys will manage it for you

Threat landscape

- Speed and sophistication of attacks using AI
- Increase in fraud – enabled by AI
- Expanded attack surface (cloud, IoT, remote work)




DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com

Our Customer's Challenges

CUSTOMER

- Lack of resources
- Lack of insight and control – discipline
- Reactive cybersecurity
- New and existing regulatory requirements
- Challenges with measuring and reporting

THREAT ACTOR

- Phishing
- Ransomware
- Software vulnerabilities
- Attacks via the supply chain
- Misconfigurations in the cloud

What can we do to protect the business?

This is the real “advanced security” that most organizations need:

Basic Hygiene

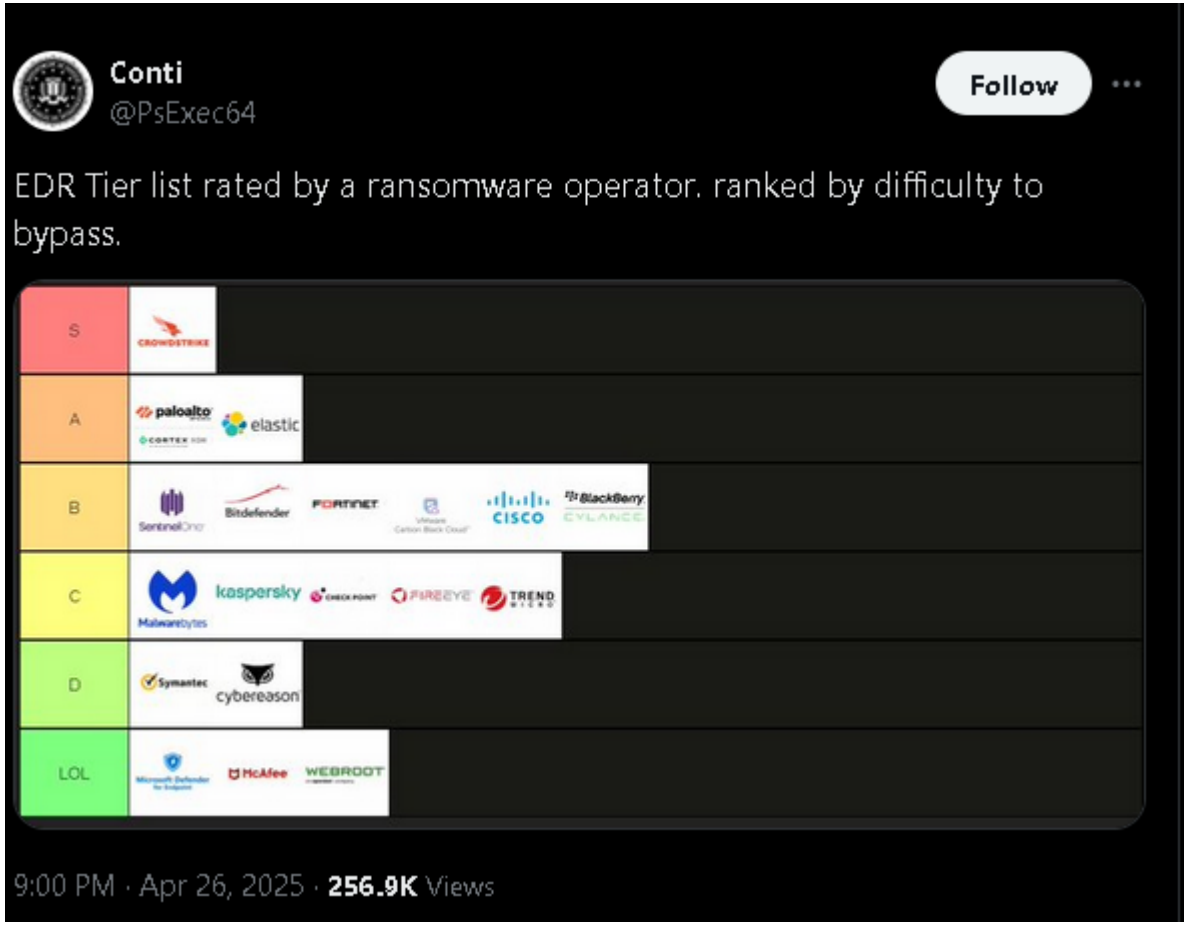
Actual Fixes

Ruthless Simplification

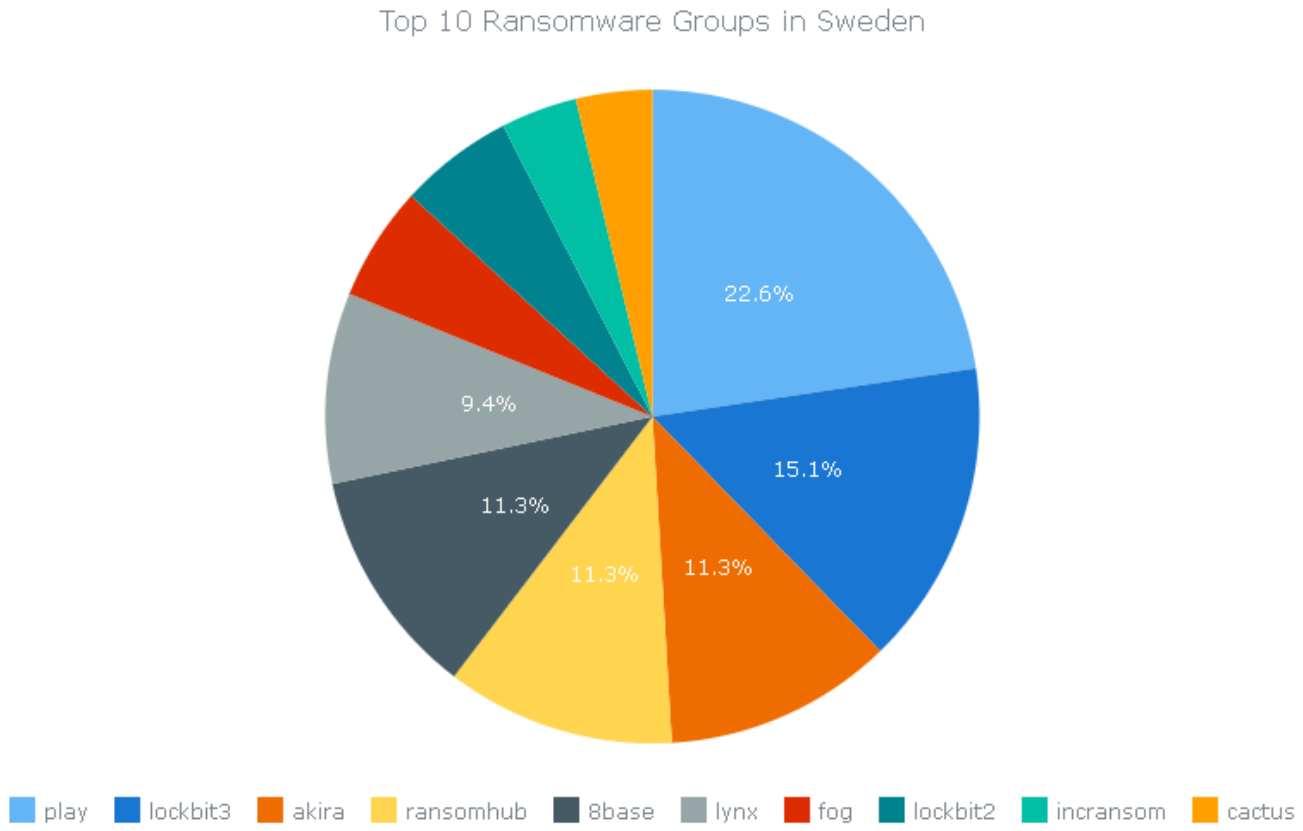
But Why do we need to do more?! We bought an 'antivirus program' (EDR, XDR, FDR, FEP…..)

Acronym	Product Name	Vendor
ATP	Advanced Threat Protection	Microsoft, Symantec
EDR	Endpoint Detection and Response	Generic/Industry term
MDE	Microsoft Defender for Endpoint	Microsoft
CDE	CrowdStrike Detection and Response	CrowdStrike
XDR	Extended Detection and Response	Multiple Vendors
NGAV	Next-Generation Antivirus	Multiple Vendors
TDR	Threat Detection and Response	Cisco Secure Endpoint
ESET	ESET Endpoint Detection and Response	ESET
CB	Carbon Black	VMware
SEP	Symantec Endpoint Protection	Broadcom
TRE	Trend Micro Endpoint	Trend Micro
SES	Sophos Endpoint Security	Sophos
EPP	Endpoint Protection Platform	General term
FDR	Falcon Detection and Response	CrowdStrike

But Why do we need to do more?! We bought an antivirus program (EDR, XDR, FDR, FEP…..)



Ransomware LIVE - www.ransomware.live



Ransomware LIVE - www.ransomware.live

DEMO- “The Wall Of Shame”

https://www.ransomware.live/map/se

Columbus Vulnerability Management Program

Comprehensive Coverage of Attack Vectors – cover every corner of your digital environment

Attack Surface Management - Stay informed about your attack surface to ensure it is fully covered.

Smart Threat Intelligence

Deliver a single source of truth - A single view of all risks for effective prioritization and action.

Columbus Vulnerability Management Program

- Scan infrastructure for vulnerabilities
- Leverage our extensive knowledge of vulnerabilities
- Generate a report

- Identify Severity
- Identify actively exploited vulnerabilities – extra critical
- Trends
- New discoveries

- Measure Exposure
- Potential Impact
- Suggest preventive security controls and mitigations
- Supply chain risks

- Set and manage deadlines
- Reach out to responsible roles and vendors
- Follow up on agreed schedule

- Action list
- Quick wins – low hanging fruit
- Most critical risks and impact
- Limitations
- Risk appetite

Columbus Vulnerability Management Program

🔍 **Continuous risk overview:**🌓 Provides real-time insight into vulnerabilities across systems, networks, and applications.	⚙️ **Proactive threat minimization:**🌓 Identify and remediate vulnerabilities before they are exploited by attackers.
📊 **Improved compliance and reporting.:**🌓 Meet requirements from standards and regulations (e.g., ISO, NIST, GDPR) with traceable processes.	⏱️ **Faster response time:**🌓 Prioritize and manage critical vulnerabilities effectively.
🧠 **Enhanced security level:**🌓 Reduce the attack surface through regular scanning and patching.	💸 **Kostnadsbesparingar genom riskreducering:**🌓 Prevent data breaches and downtime, reducing recovery costs.

🤝 **Strong team collaboration: Creates better coordination between IT, security, and operations teams.**

Columbus

5 Steps to Successful Vulnerability Management

1. **Automation & Continuity -** Automate scans and processes to ensure continuous and effective protection.

2. **Risk-Based Approach** - Prioritize vulnerabilities based on business risks and simple key metrics like CVSS and system criticality.

3. **Realistic Ambition Level & Insight** - Set clear goals. Use the Q10 method: identify and fix 5–10 critical vulnerabilities per quarter.

4. **Involve & Engage** - Security is a team effort. Involve system owners, developers, CISOs, and IT managers. Integrate with existing tools.

5. **REMEMBER DAVE from slide 11?!- Strengthen the Human Firewall** - Users are often the weakest link – train them through simulated attacks and ongoing security awareness.

NIS & NIS2 – Träder i kraft den 18:e Oktober 2025

Essential Entities

- Energy Sector
- Wastewater
- Healthcare Sector
- Drinking Water Supply & Distribution
- Banking Sector
- Financial Market Sector
- Digital Infrastructure
- Transport Sector
- Space
- Public Administration

Important Entities

- Waste Management
- Digital Distributors
- Postal & Courier Services
- Chemicals Production, Processing & Distribution
- Production & Manufacturing
  - MedTech Products
  - Computers, electronics, and Optics
  - Electrical Appliances
  - Industrial Machines
  - Motor Vehicles
  - Other transports
- Food Production, Processing & Distribution

Columbus

CYBER EUROPE enisa CYBER EUROPE

Demands/impact:	Our solution:
A systematic, analytical, risk-based work within information security and perform risk assessments.	Automated and continuous risk assessments.
Report Incident reporting – also for exposure without an incident.	Discover vulnerabilities and generate reports.
Be able to demonstrate compliance today and historically.	Reports that shows compliance today and historically.
Administrative sanctions; lost permits, certifications and similar.	Proactively strengthen your cyber defense to avoid incidents.
Personal responsibility for top management.	Proactively strengthen your cyber defense to avoid incidents.

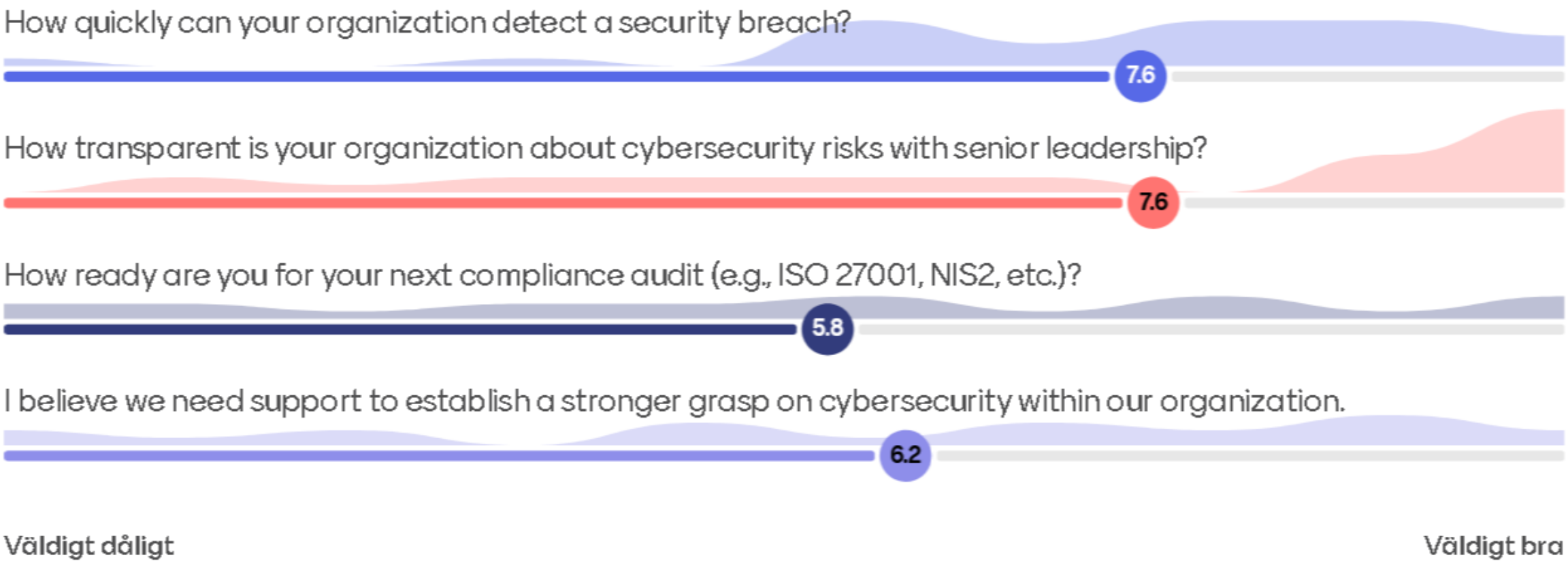
A few questions

How are you doing?

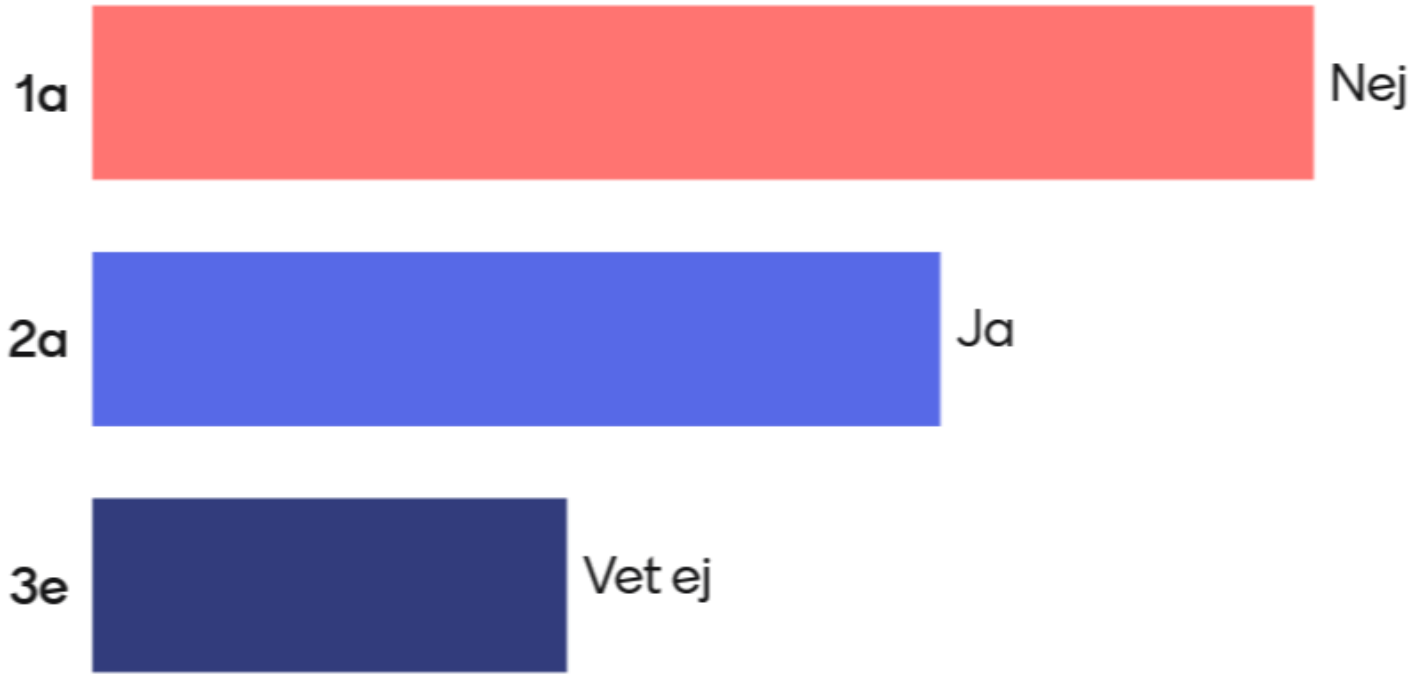
What is the most *"unsafe"* thing you've ever done online – honestly?

Använt samma lösenord	Shopping	Unsafe password
Öppnat fel mail.	123456	Bjet
Bad password	Downloaded	Använt samma lösenord
Same password everywhere	Samma lösenord jämt	Same password on multiple sites
Dejtade	Same password on different pages	Klickat på phisinglänkar

On a scale from 1 to 10



Have you experienced a cybersecurity incident in the past year?



NIS & NIS2 – Takes effect on October 18, 2025

Essential Entities

- Energy Sector
- Wastewater
- Healthcare Sector
- Drinking Water Supply & Distribution
- Banking Sector
- Financial Market Sector
- Digital Infrastructure
- Transport Sector
- Space
- Public Administration

Important Entities

- Waste Management
- Digital Distributors
- Postal & Courier Services
- Chemicals Production, Processing & Distribution
- Production & Manufacturing
  - MedTech Products
  - Computers, electronics, and Optics
  - Electrical Appliances
  - Industrial Machines
  - Motor Vehicles
  - Other transports
- Food Production, Processing & Distribution

Demands/impact:	Our solution:
A systematic, analytical, risk-based work within information security and perform risk assessments.	Automated and continuous risk assessments.
Report Incident reporting – also for exposure without an incident.	Discover vulnerabilities and generate reports.
Be able to demonstrate compliance today and historically.	Reports that shows compliance today and historically.
Administrative sanctions; lost permits, certifications and similar.	Proactively strengthen your cyber defense to avoid incidents.
Personal responsibility for top management.	Proactively strengthen your cyber defense to avoid incidents.

Columbus

Albert Altman
Principal Security Consultant
076 760 54 80
albert.altman@columbusglobal.com

Feeling overwhelmed? Contact us, and we'll go through everything together.