Making informed decisions using real-time data

EY Cybersecurity health check

Building a better working world

The foundation to a Secure-by-Design approach

Every internet-connected business is a target for cybercrime. Cyber attackers are becoming more sophisticated, using more advanced phishing and malware techniques to find weak points in organizations large and small, in public and private sectors alike.

These attacks are leading to increased spend on preventative and detective security technology, but these same organizations are not always getting their planned return on investment.

> “Only 10% of organizations say they are able to quantify the effectiveness of their cybersecurity measures in financial terms.

The Chief Information Security Officer of today needs to work collaboratively with the business, if not they will inevitably be side-stepped by other functions and lines of business which could expose the business to new threats. Cybersecurity needs to be embedded into business initiatives – creating a culture of Security by Design.

This ‘Secure-by-Design’ approach starts with getting the basics right and putting in place the foundations to embed cybersecurity across the business. Establishing robust cyber hygiene, knowing what your assets are and how they are protected is the starting point to building trust across the organization.

Increase trust with a real-time view of data

Many cybersecurity leaders already say that the most challenging aspect of their role is proving the value of what they do and securing the budget they believe they require. For many, this is more difficult than actually managing security – even when it comes to evolving technologies and new threats.

Organizations are making large investments in risk and controls optimization, and rightly so. Many of these investments are based on qualitative data, industry benchmarks and maturity assessments.

However, to build trust, you need to make informed and risk-based decisions using a blend of qualitative *and* quantitative data sets.

The maturity assessment is still a powerful tool that a leader can use, helping relay findings and key messages to an executive audience. However to make the right decisions cybersecurity leaders need meaningful and actionable data regarding their increasingly complex digital ecosystems.

Figure 1 – CISO Budget Requests– EY GISS 2020

How EY teams provide that real-time view

EY's approach to cyber risk management focuses on business alignment with people, processes and technology to manage cyber risk in the organization. We understand the organization's risk exposure via a data-driven approach supported by actionable data.

The EY assessment provides a real-time view of the organization's digital ecosystem, reviewing the active security controls and understanding the risk posture through areas such as patch and vulnerability findings.

The EY solution enriches your existing systems with accurate real-time endpoint data.

Identifying what assets an organization has, where they have exposed assets, finding unauthorized back door accounts, seeing open file share which can aid lateral movement and determining who is synchronizing data into personal cloud sharing accounts to name a few.

Speed

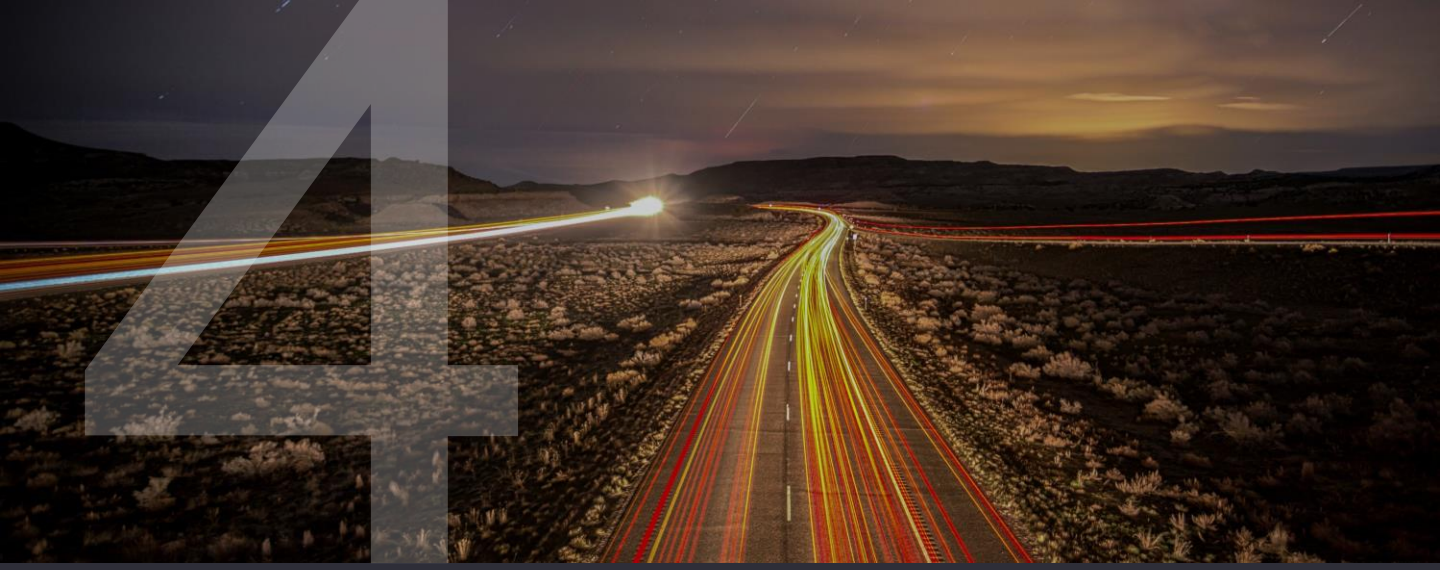
Technically, there is a single agent with minimal infrastructure. Operationally, we have one common console that harmonizes IT Ops and Security around one actionable source of data.

Visibility

The solution tells you what processes are running on your end points right now. Being able to investigate your entire network in real-time is critical to building contextual insights.

Control

The solutions scale at speed, allowing you to confidently take action, such as issuing a patch, deploying a software update, or resolving configuration drift.



Findings that can be used to drive further investment

The EY Cybersecurity health check output will detail the assessment approach, the scope (typically <5,000 enterprise endpoints) and the detailed findings. Example findings from previous assessments have included:

On average the health check finds:

- 12-20% unmanaged endpoints
- 5-20% missing or broken agents
- 60% of Managed Devices missing 6+ critical Patches
- Out of date software on most devices

Focusing on Return on Investment

Discover, retire and reduce total cost of ownership through properly managed devices	Simplify reporting and distribution, and inform stakeholders with an accurate picture of the risk position	Attack surface reduction, avoiding risk of compromise and significant business disruption	Simplify Technology management infrastructure

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

The global EY organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity's acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

EY's organization is represented in Switzerland by Ernst & Young Ltd, Basel, with 10 offices across Switzerland, and in Liechtenstein by Ernst & Young AG, Vaduz. In this publication, "EY" and "we" refer to Ernst & Young Ltd, Basel, a member firm of Ernst & Young Global Limited.

ED None

ey.com/ch

If you were under cyber attack, would you ever know?

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless. When one tactic fails, they will try another until they breach an organization's defenses.

At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our ecosystems of digitally connected entities, people and data increase the likelihood of exposure to cybercrime in both the work and home environment. Even traditionally closed operational technology systems are now being given IP addresses, enabling cyber threats to make their way out of back-office systems and into critical infrastructures such as power generation and transportation systems.

For EY Consulting, a better working world means solving big, complex industry issues and capitalizing on opportunities to As better-connected consultants, EY teams help EY clients thrive in the Transformative Age.

Being better-connected lies at the heart of EY Advisory and how we work. It is about bringing together the talents, creativity and experience of the entire organization and alliances. It refers to the way we collaborate with each other, EY clients, market influencers and strategic alliances globally to help the clients realize sustainable results and build a better working world.

Combining a complete understanding of the clients' priorities, such as strategy, digital, technology, analytics, cybersecurity and people, with competencies in performance improvement, risk and people advisory services.

In an era that presents unprecedented change with limitless opportunity, success in the Transformative Age requires boldness, confidence and leadership to seize the opportunities and rise to the challenges of this new age.

By asking the better questions and finding answers to some of the world's toughest challenges, EY Advisory is helping to build a better working world.

**The better the question. The better the answer.
The better the world works.**

Your key contacts

Tom Schmidt
EMEIA Financial Services Cybersecurity Competency Leader | Cybersecurity Leader Financial Services, Switzerland
tom.schmidt@ch.ey.com
Mobile: +41 79 558 42 08
Office: +41 58 286 64 77

Roman Haltinner
Cybersecurity Competency Leader Europe West, Switzerland
roman.haltinner@ch.ey.com
Mobile: +41 79 886 08 36
Office: +41 58 286 38 00

Sibel Kolb
Senior Manager | Cybersecurity Financial Services, Switzerland
sibel.kolb@ch.ey.com
Mobile: +41 79 938 76 46
Office: +41 58 289 63 96