Path to cyber resilience: Sense, resist, react

Results and relevant insights for the health care sector

EY
Building a better working world

?!

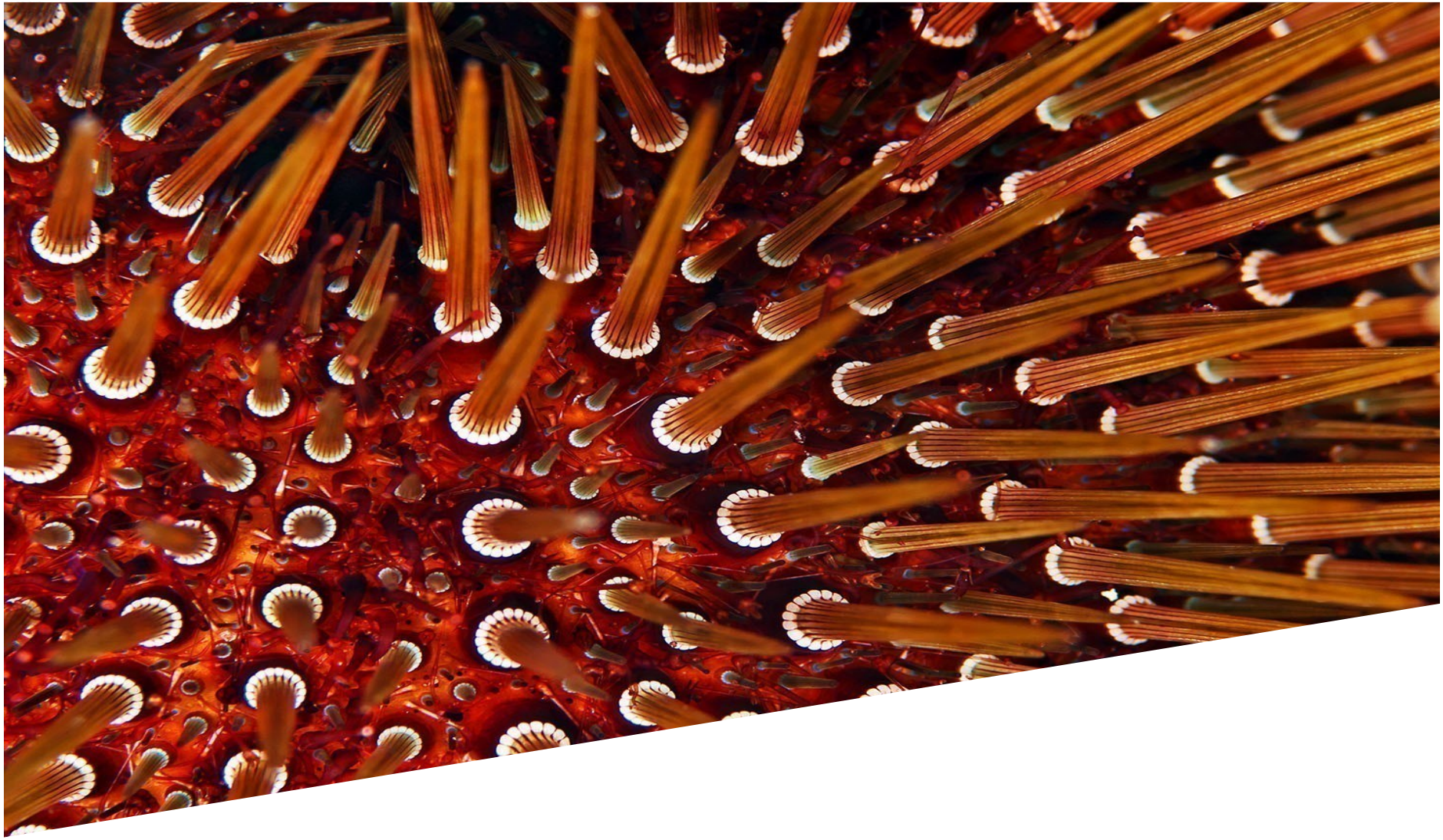

3D
1010110
1001001
1101010
WWW
IOT

The Art of War

*It is said that if you **know your enemies** and **know yourself**, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.*

Sun Tzu
*(Chinese general, military strategist, and author of "**The Art of War**")*

The state of cyber resilience



The high-level components of cyber resilience

Sense

The ability of organizations to predict and detect cyber threats.

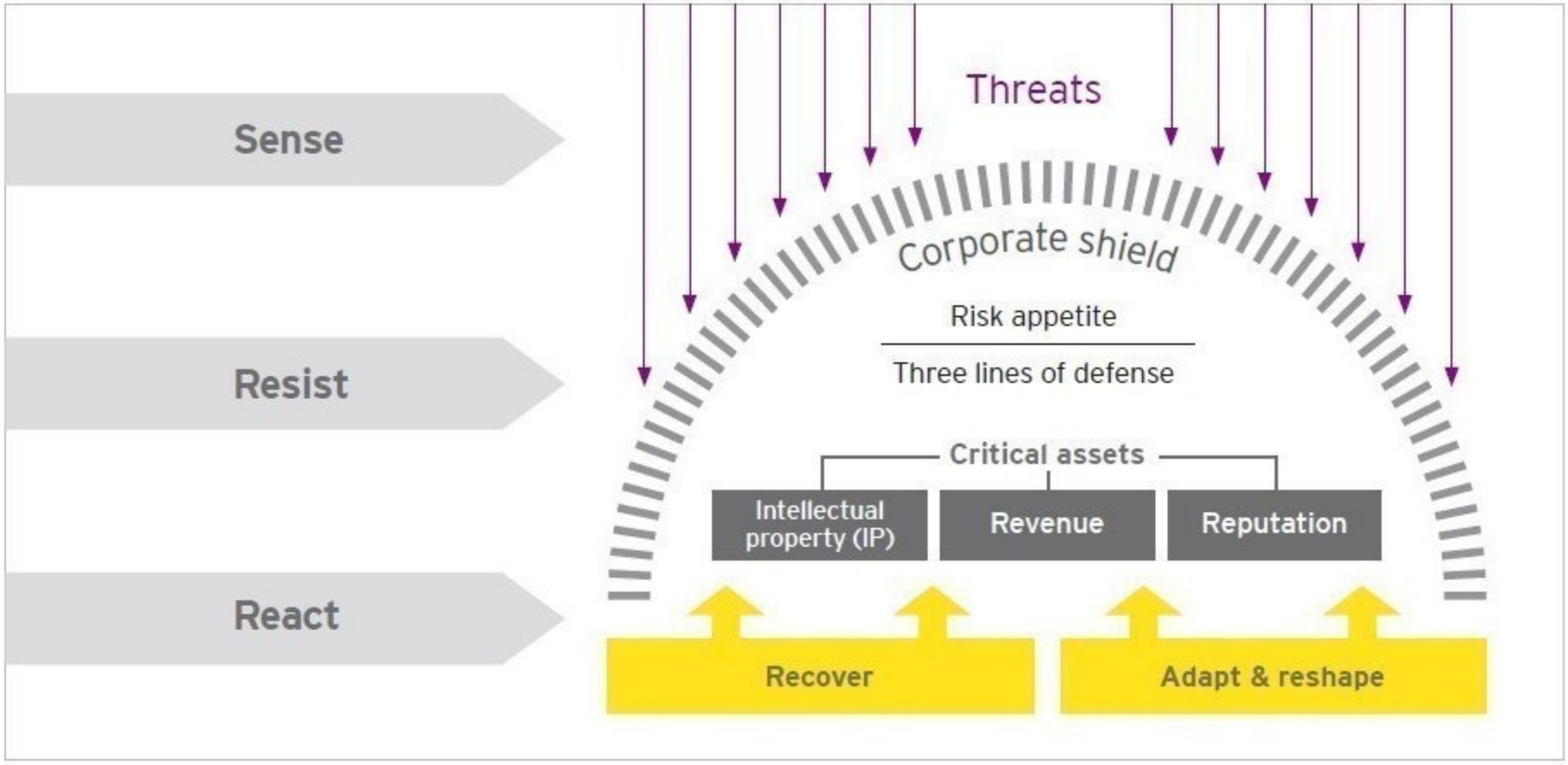
Resist

The corporate shield, starting with how much risk an organization is prepared to take, followed by three lines of defense.

React

Being ready to deal with the disruption, with incident response capabilities, crisis management, preservation of evidence and investigation of the breach.

Cyber resilience



The overall picture

	Sense (See the threats coming)	Resist (The corporate shield)	React (Recover from disruption)
Where do organizations place their priorities?	Medium	High	Low
Where do organizations make their investments?	Medium	High	Low
Board and C-level engagement	Low	High	Low
Quality of executive or boardroom reporting	Low	Medium	Low

EY's Global Information Security Survey

- EY's 19th Global Information Security Survey (GISS) captures the responses of 1'735 C-suite leaders and Information Security and IT executives/managers, representing most of the world's largest and most-recognized global companies.

- Responses were received from 72 countries and across nearly all industries.

- In Switzerland, we had 49 participants, of which 31 stem from the financial services sector (banks, asset managers and insurance companies), 4 from the life sciences sector, 4 from the technology sector and 3 from the government & public sector.

- In the Life Sciences sector, we had 29 participants, in the Healthcare sector we had 69 participants globally.

GISS demographics

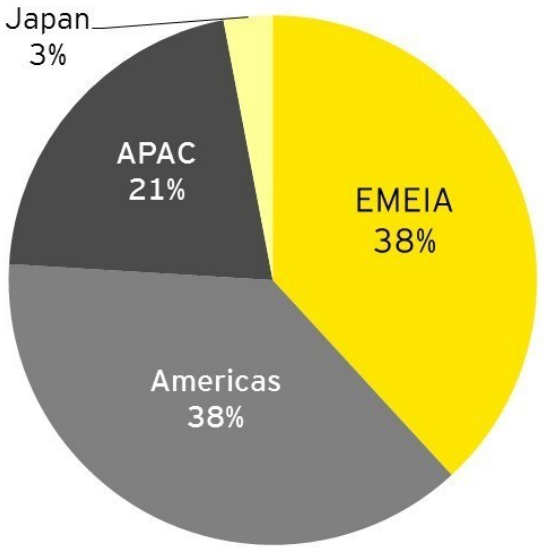
1'735

respondents

25

industry sectors

Respondents by area
(1'735 respondents)



Insights for the health care sector

A high level of confidence?

- Organizations have improved their Sense capabilities significantly, using:
  - Cyber threat intelligence
  - Installing continuous monitoring mechanisms, such as a security operations center (SOC)
  - Identifying and managing vulnerabilities
  - Installing active defense

- But not enough organizations are delivering the basics:

44%

LS: 35% / HC: 53%

do not have an SOC.

64%

LS: 54% / HC: 72%

do not have, or only have an informal, threat intelligence program.

Securing your ecosystem

- In the digital, connected world, events in an organization's network of suppliers, customers, and government bodies (i.e., the ecosystem) can go on to impact the organization itself. This is a major area of risk which is often overlooked:
  - **68%** would not increase their information security spending even if a supplier was attacked
  - **58%** would not increase their spending if a major competitor was attacked
- An organization's sensory system is much stronger when events in its ecosystem are taken into account

Focus on cyber risks, not only on cybersecurity

- Organizations have improved their abilities to resist attacks, but attacks take different and increasingly complex forms
- Executing control measures in the corporate shield may work against DDoS or virus attacks, but not against sophisticated, persistent attacks that dedicated and organized cyber criminals are launching every day

  - In 2015, **88%** said their cybersecurity function did not fully meet their organization's needs
  - In 2016, it is **86%**, which is not a notable improvement

Where should organizations focus to better resist today's attacks?

Activate your defences

- Resisting, defending, mitigating and neutralizing attacks is the necessary core of cybersecurity.
- The services and tools organizations use have mostly kept pace, although 57% say they have had a recent significant cybersecurity incident which shows the corporate shield needs more strength.
- Maturity levels are too low. Percentage who say their management processes are mature:

Software security:	**29%**
Security monitoring:	**38%**
Incident management:	**38%**
Identity and access management:	**38%**
Network security:	**52%**

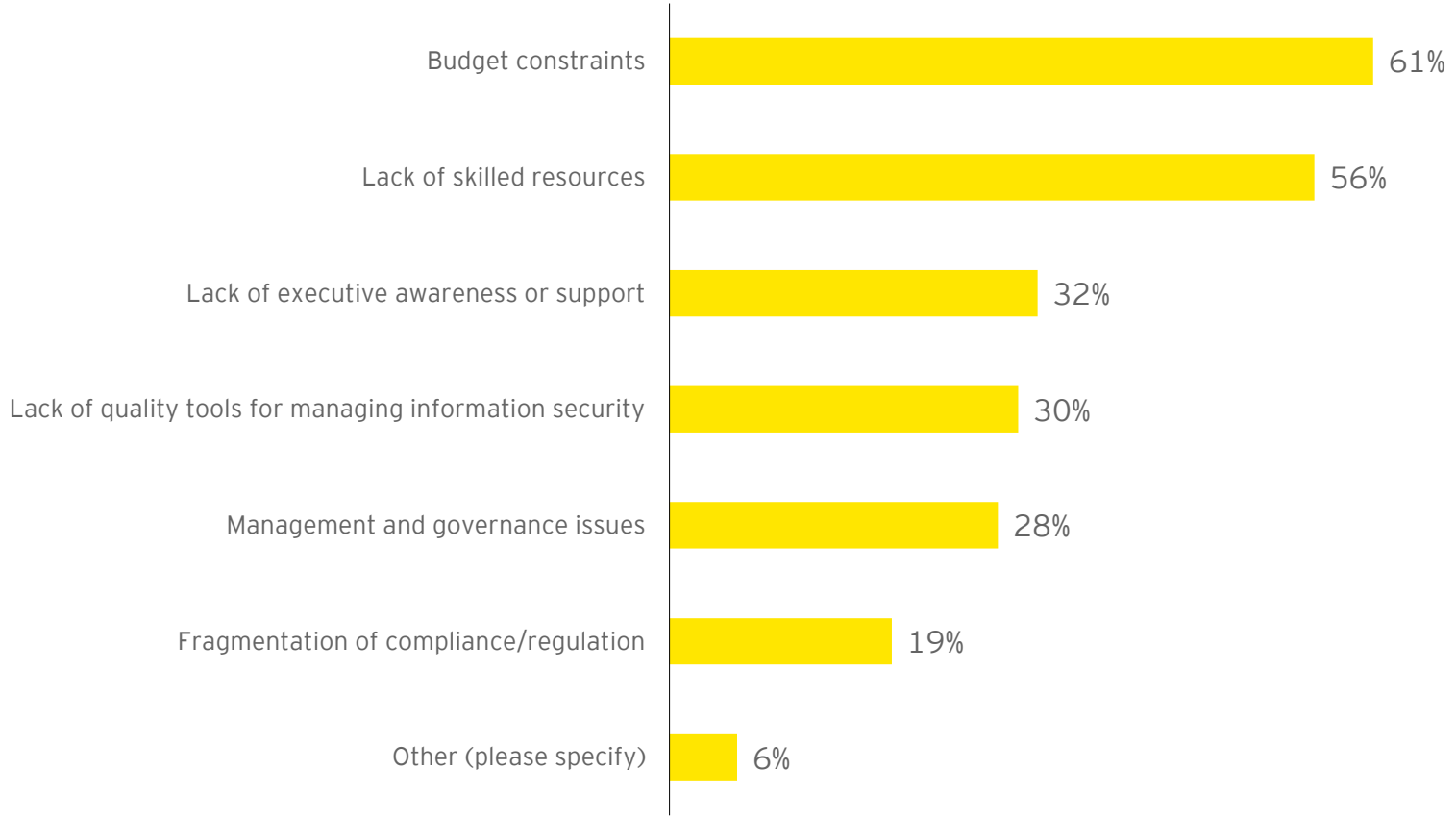
Where should organizations focus to better resist today's attacks? cont'd

Take an unorthodox approach

- Defenses are usually seen as hard barriers, but there are other ways organizations can minimize the impact of an attack:
  - **Switching from fail-safe to safe-to-fail:** Organizations have been right to build robust, resilient fail-safe operations, but it can no longer be the only option. The new aim should be safe-to-fail, so that on sensing a threat, mechanisms absorb the attack, reduce the velocity and impact and accept partial system failure as a way to limit the damage
  - **From protection to sacrifice:** Technologies today make it possible to sacrifice portions of information or operations, which can be performed as an automated response. When the SOC recognizes a high-level threat, the system owner receives an alert and the system is shut down

What are the main obstacles or reasons that challenge your Information Security operation's contribution and value to the organization?

(Select all that apply)



Multiple responses allowed

The impact of the internet of things (IoT)

Challenges related to the number of devices which will become part of the network in a very short period of time. Key concerns cited are:

46% (LS: 48% / HC: 60%) say their ability to know all their assets

43% (LS: 41% & HC: 46%) say keeping devices bug free

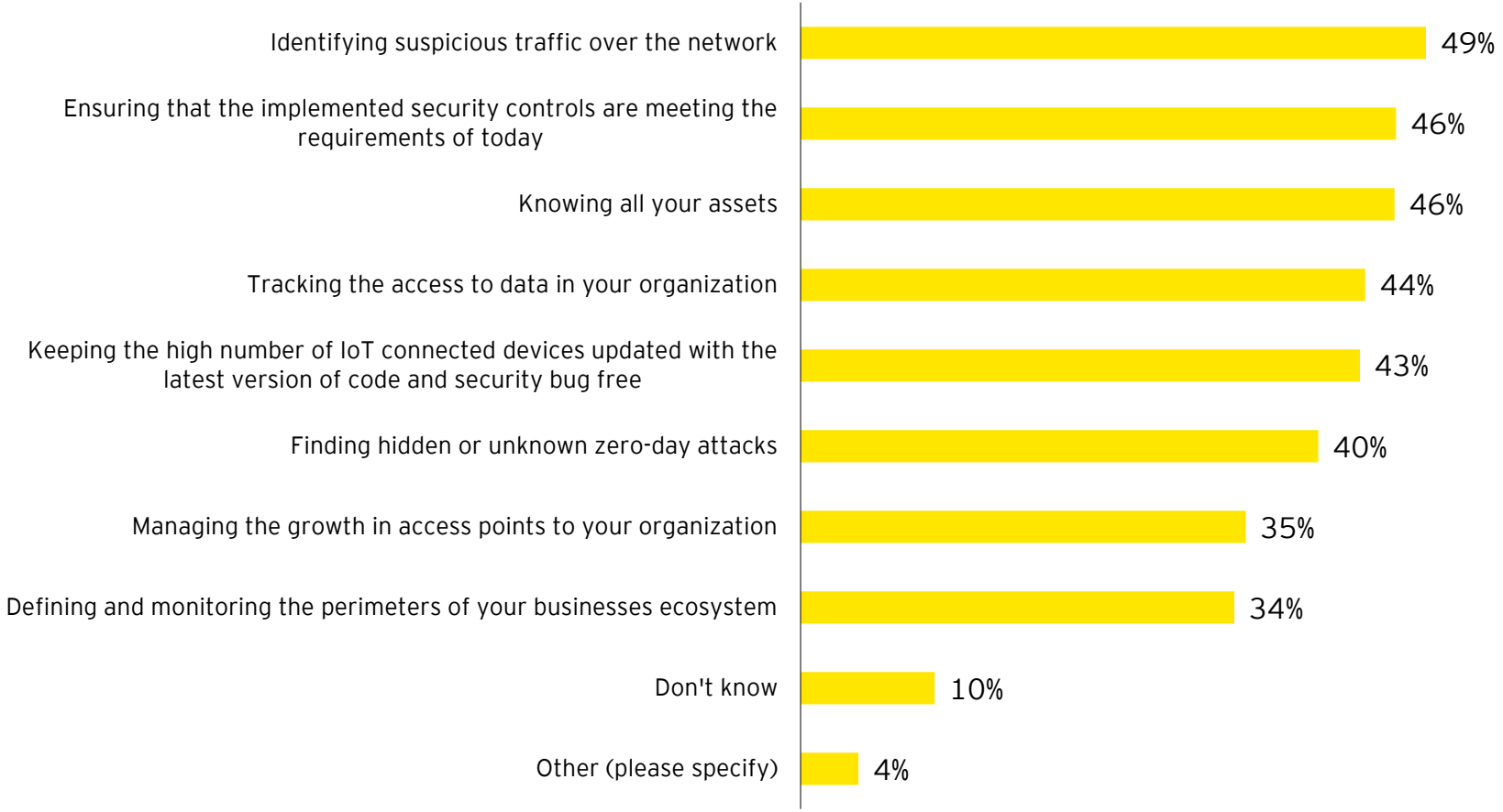
43% (LS: 52% / HC: 56%) say patching vulnerabilities fast enough

The impact of the internet of things (IoT)
cont'd

- Challenges related to the size of the data traffic
  - Organizations doubt they are going to be able to continue to:
    - Identify suspicious traffic
    - Track who has access to their data
    - Be able to find hidden and unknown zero-day attacks
- Challenges related to the ecosystem
  - The ecosystem will grow significantly as connectivity expands and the volume of data increases
  - It will become difficult to identify what part of the ecosystem is going to impact the organization, more so if the organization's own cybersecurity is fragmented and not joined up
    - **34% (LS: 41% / HC: 37%)** expect difficulties monitoring the perimeter of their ecosystems

What do you consider to be the information security challenges of the IoT for your organization?

(Select all that apply)



Multiple responses allowed

Information sharing and collaboration are on the rise

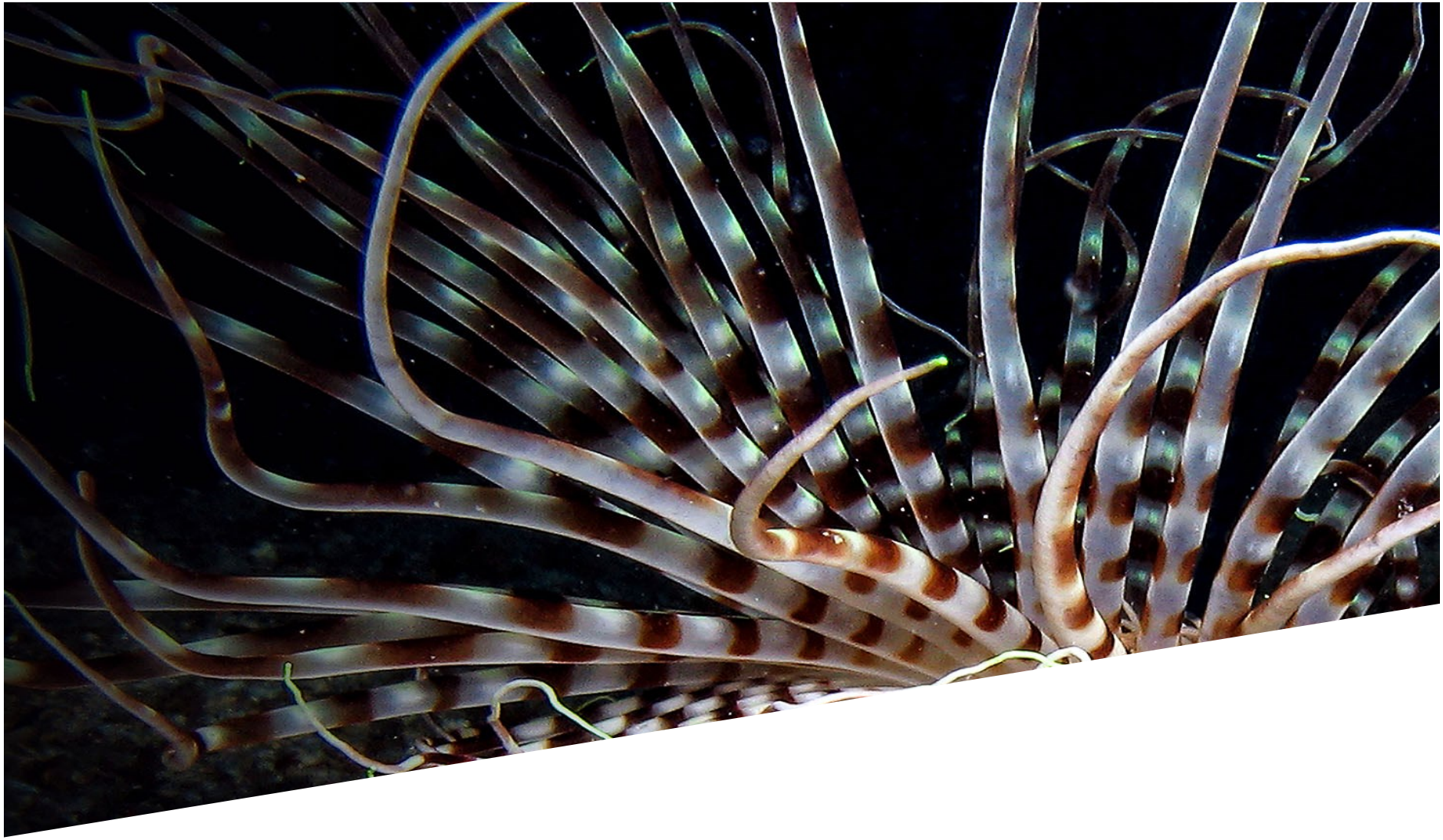
- Governments and other entities are increasingly concerned with cybersecurity. Industry-specific regulations relating to cyber risks are gathering momentum.
- Standards are being developed for critical infrastructure organizations; greater calls for information sharing, collaboration and mandatory reporting
- It should be anticipated this will become compulsory

49%

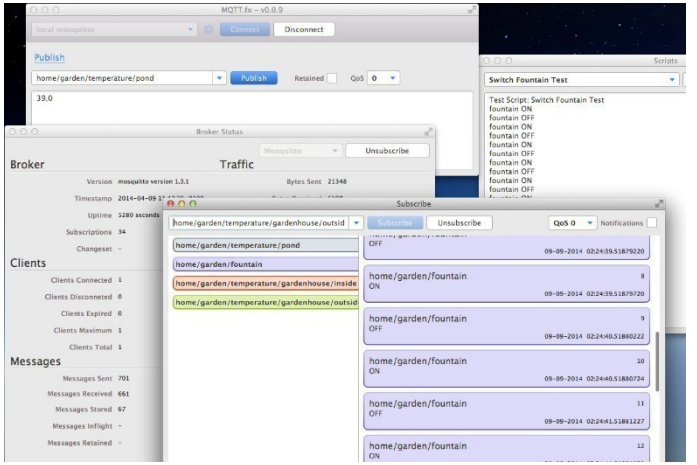
of our respondents' SOCs collaborate and share data with others in the same industry.

LS: 90% / HC: 43%

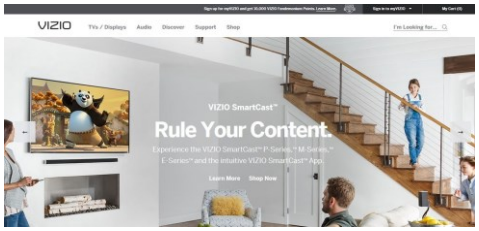
Current developments that are affecting the health care sector



IoT is the new field of play for cyber attackers

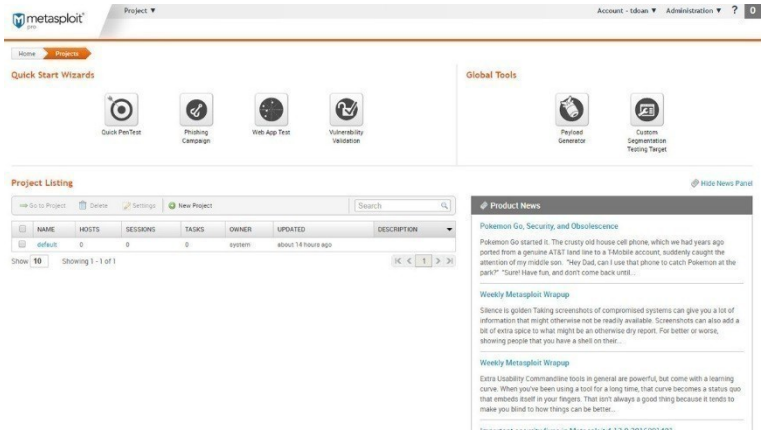


VIZIO



Cyber attackers are relying on standard components

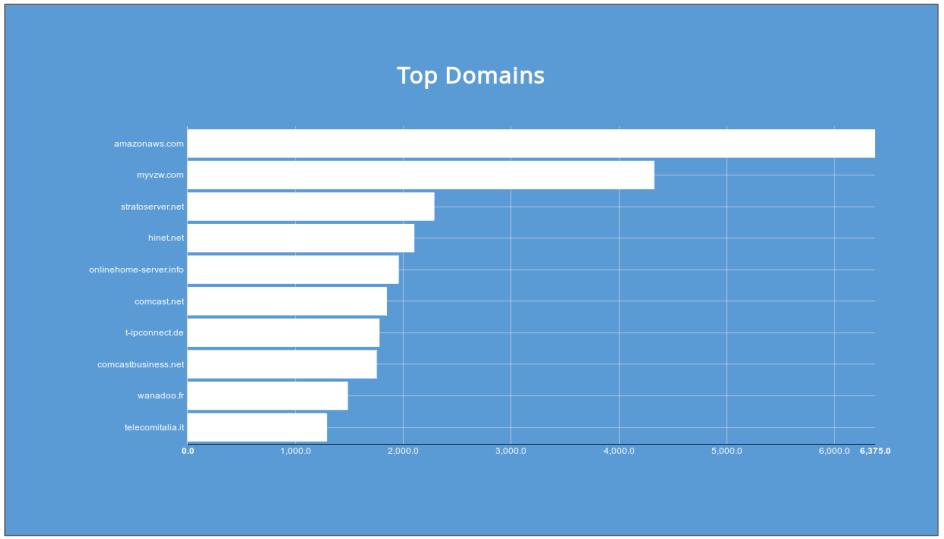
metasploit

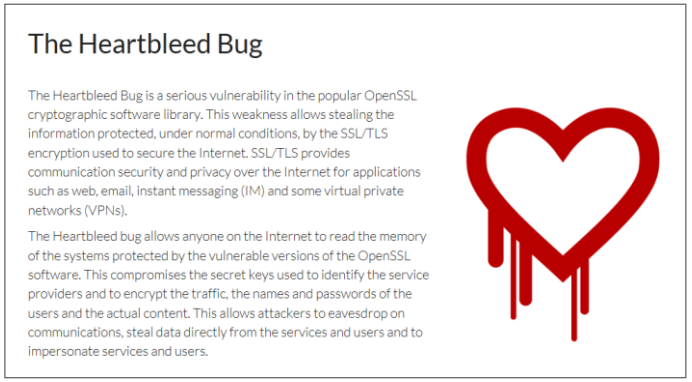


Metasploit

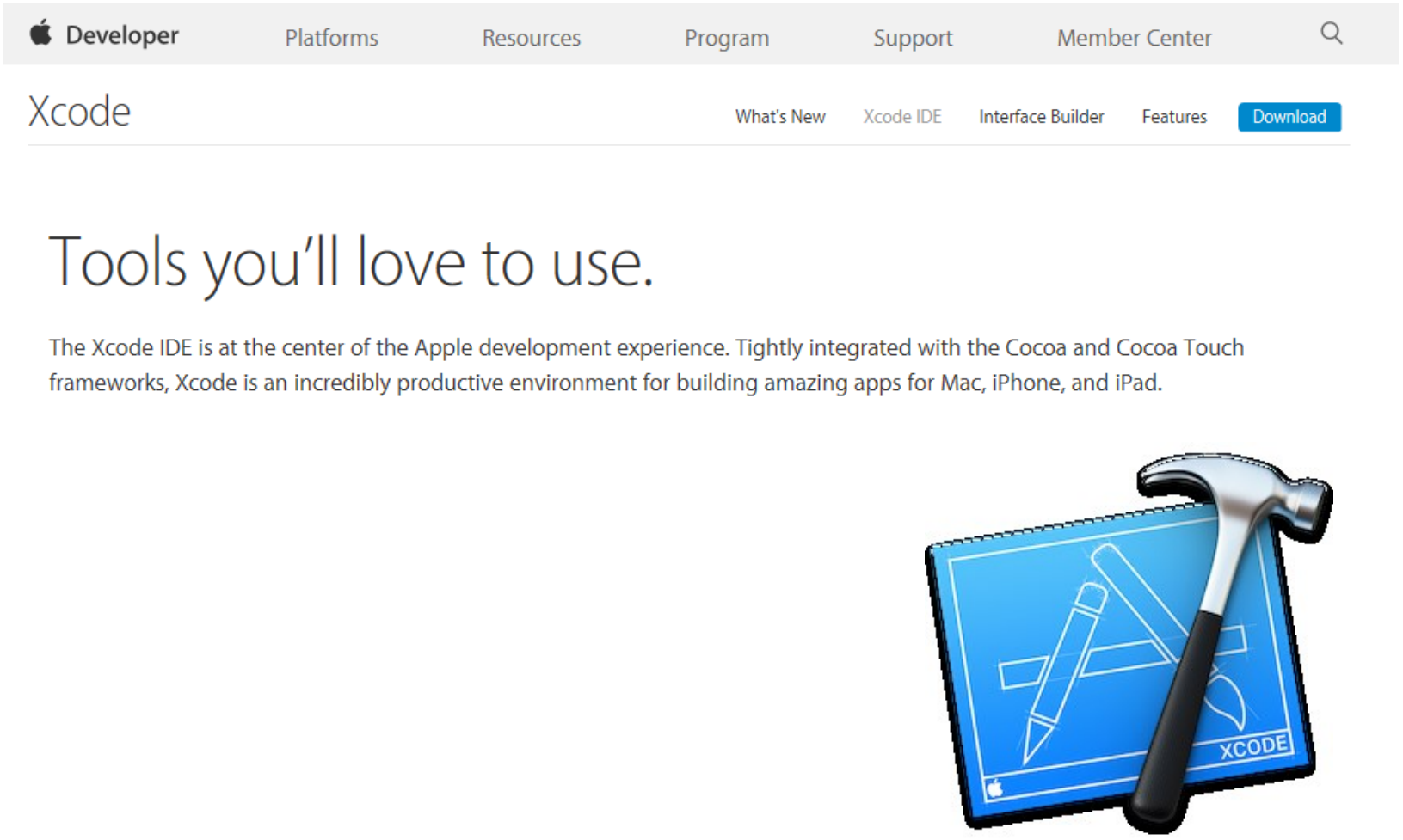
Hardware Bridge API

Critical vulnerabilities are not going to disappear, not even after much time has passed





Developers are under cyber attack



Summary of current developments 1/2

- Cybercrime in general is on the rise – target data sets are broadening (e.g., financial data, personal data, voter data, fraud)
- The Internet of Things (IoT) is the new playing field for attackers of all kinds – as targets as well as for attacking other infrastructure (various device types are being targeted; Raspberry Pi is increasingly used as attack platform; sensors will be in focus going forward)
- The figures and volumes on the black market are increasing (Adobe Flash 0-day exploits are traded for > 100,000 USD, Apple IOS 0-day exploits are traded for > 1,000,000 USD)
- As a result, more and more companies are setting up bug bounty programs
- The (known) damage following cyber attacks is increasing

Summary of current developments 2/2

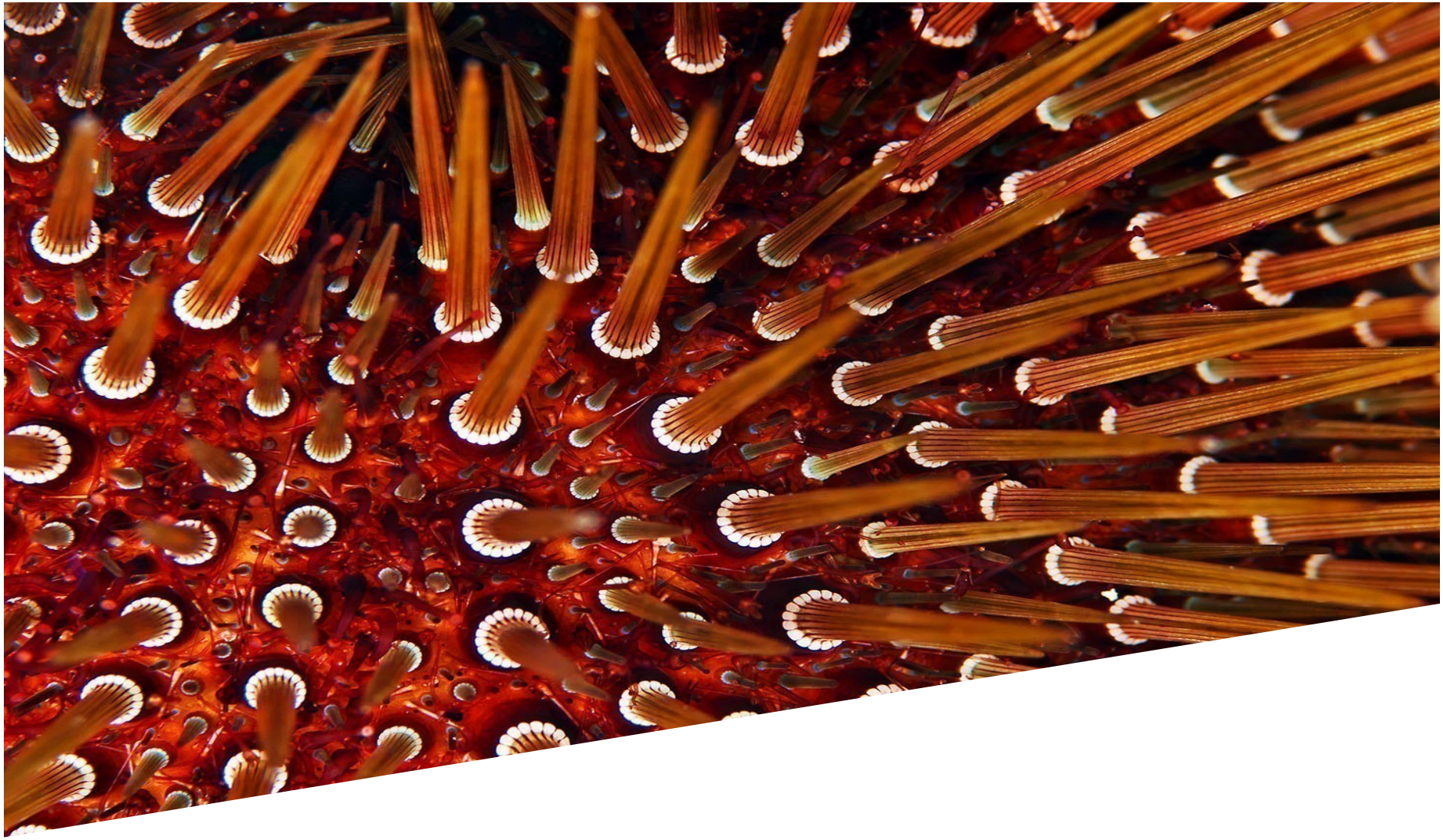
- Attackers are using more and more standard components and tools that are also used by administrators (e.g., PowerShell, metasploit)
- Trust relationships of apps will increasingly come under attack (e.g., XcodeGhost)
- Developers will be increasingly targeted (backdoors in source code, compiler, development environment) -> should be increasingly in focus of audit functions
- Due to large scale deployment, mobile or IoT platforms are increasingly interesting for attackers – and there are 0-day exploits to be expected, often without the possibility to patch (e.g., "stagefright")
- Regulators and critical infrastructure providers are issuing more requirements related to cybersecurity and especially penetration testing
- More data is being lost or stolen compared to prior years

Key aspects to consider when addressing today's cyber risks

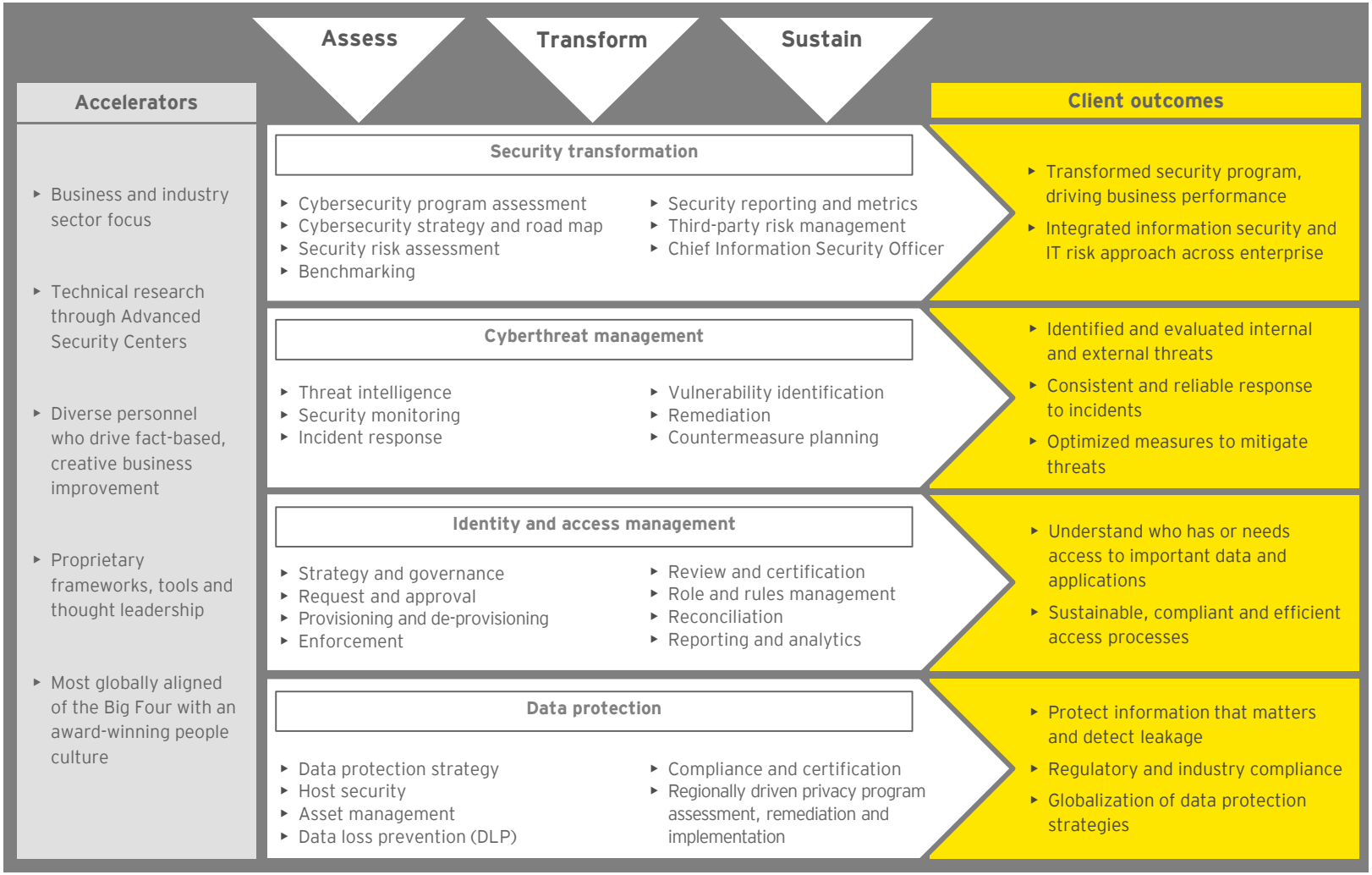
- Put stronger focus on developers and related infrastructure (access restrictions, logging)
- Understand your exposure and role within the IoT environment (User? Developer? Manufacturer? Which devices and how many?)
- Invest in meaningful threat intelligence (operational, tactical, strategic)
- Restrict access to components or tools for administrative use
- Enforce need-to-know and need-to-have principles
- Improve logging and monitoring of infrastructure and leverage a SOC solution for correlation
- Keep an eye on regulators' requirements and implement accordingly if applicable to respective industry
- Use versioning systems, offline backup and cryptographic checks for source code
- Evaluate impact of GDPR


Discussion / Q&A

EY's cybersecurity services and related insights – Appendix



EY's cybersecurity services

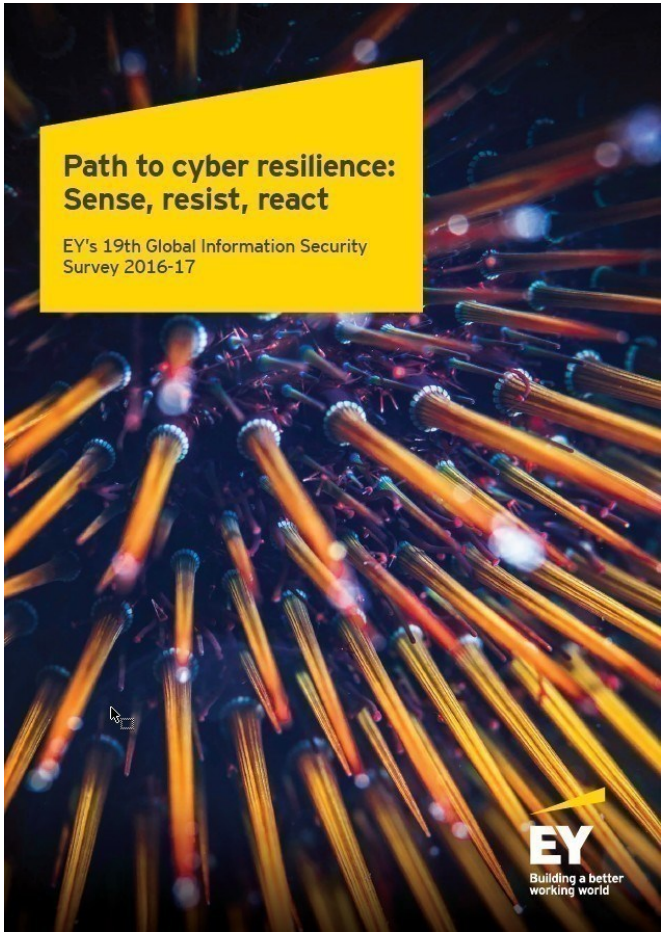


Further information and insights

See full survey report:
Path to cyber resilience: Sense, resist, react – EY's 19th Global Information Security Survey 2016-2017: www.ey.com/GISS

View more of EY's insights on cybersecurity on: www.ey.com/cybersecurity

For further GRC thought leadership, please refer to our Insights on governance, risk and compliance series on: www.ey.com/GRCinsights



EY presenter's CV

CV Stefan Wenigmann

Contact:
+41 58 286 67 56
+41 58 289 67 56
stefan.wenigmann@ch.ey.com

Follow and connect with Stefan on:
XING | LinkedIn | Twitter

Background:

- Stefan is Senior Manager in the IT Risk and Assurance (ITRA) practice, focused on Cyber- as well as Information Security.
- He joined EY in 2007 (Berne office, CH) and is currently based in the Zurich (CH) office.
- Today, he manages and performs all kinds of cybersecurity or data protection and privacy-related projects with clients across all industries. Besides his involvement in typical cybersecurity-related projects, including cybersecurity assessments, he often conducts interdisciplinary information security and data protection assessments as well as holistic cybersecurity activities and security benchmarking.
- Stefan graduated as a Dipl. Informatiker FH, Business Applications of Computer Science at HFU Furtwangen University of Applied Sciences in 2007.
- He is a Privacy and Data Protection Officer, udis Ulmer Akademie für Datenschutz und IT-Sicherheit (2005), Certified ISO 27001 Lead Implementer as well as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC) and Certified Information Systems Auditor (CISA). He is a member of the Information Systems Audit and Control Association (ISACA), the $(ISC)^2$ and a member of the Information Security Society Switzerland (ISSS).
- He speaks German (mother tongue) and English.

EY | Assurance | Tax | Transactions | Advisory

About the global EY organization
The global EY organization is a leader in assurance, tax, transaction and advisory services. We leverage our experience, knowledge and services to help build trust and confidence in the capital markets and in economies all over the world. We are ideally equipped for this task – with well trained employees, strong teams, excellent services and outstanding client relations. Our global purpose is to drive progress and make a difference by building a better working world – for our people, for our clients and for our communities.

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. For more information, please visit www.ey.com.

EY's organization is represented in Switzerland by Ernst & Young Ltd, Basel, with ten 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

www.ey.com/ch