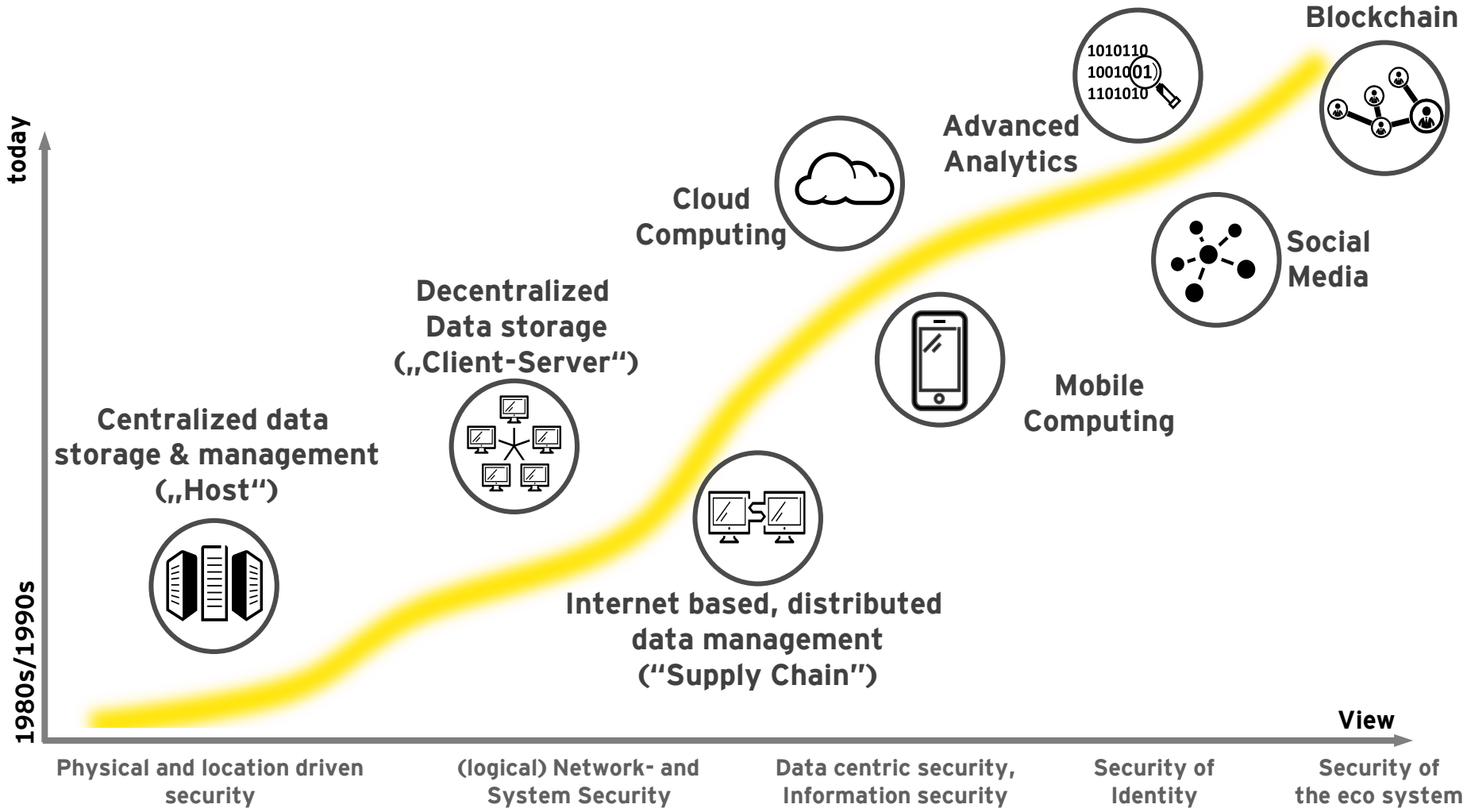
Cybersecurity & Blockchain technology: Preparing to face cyber attacks

Co-Willing Economic Development Conference

Kenia / 25-30 Jan. 2019 – Marc Minar

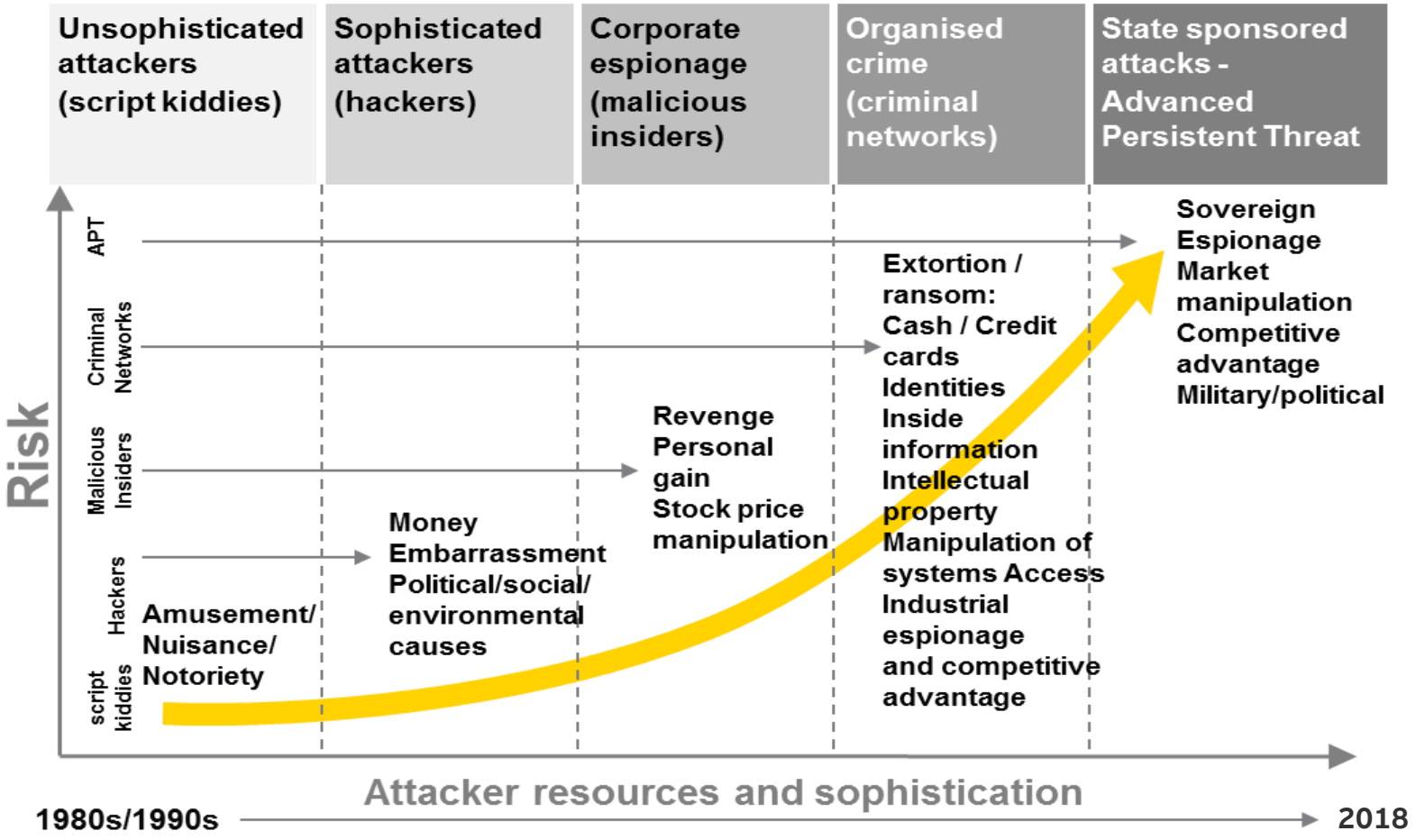
EY
Building a better working world

Cyberrisk and Cybercrime - Challenges caused due to paradigm change

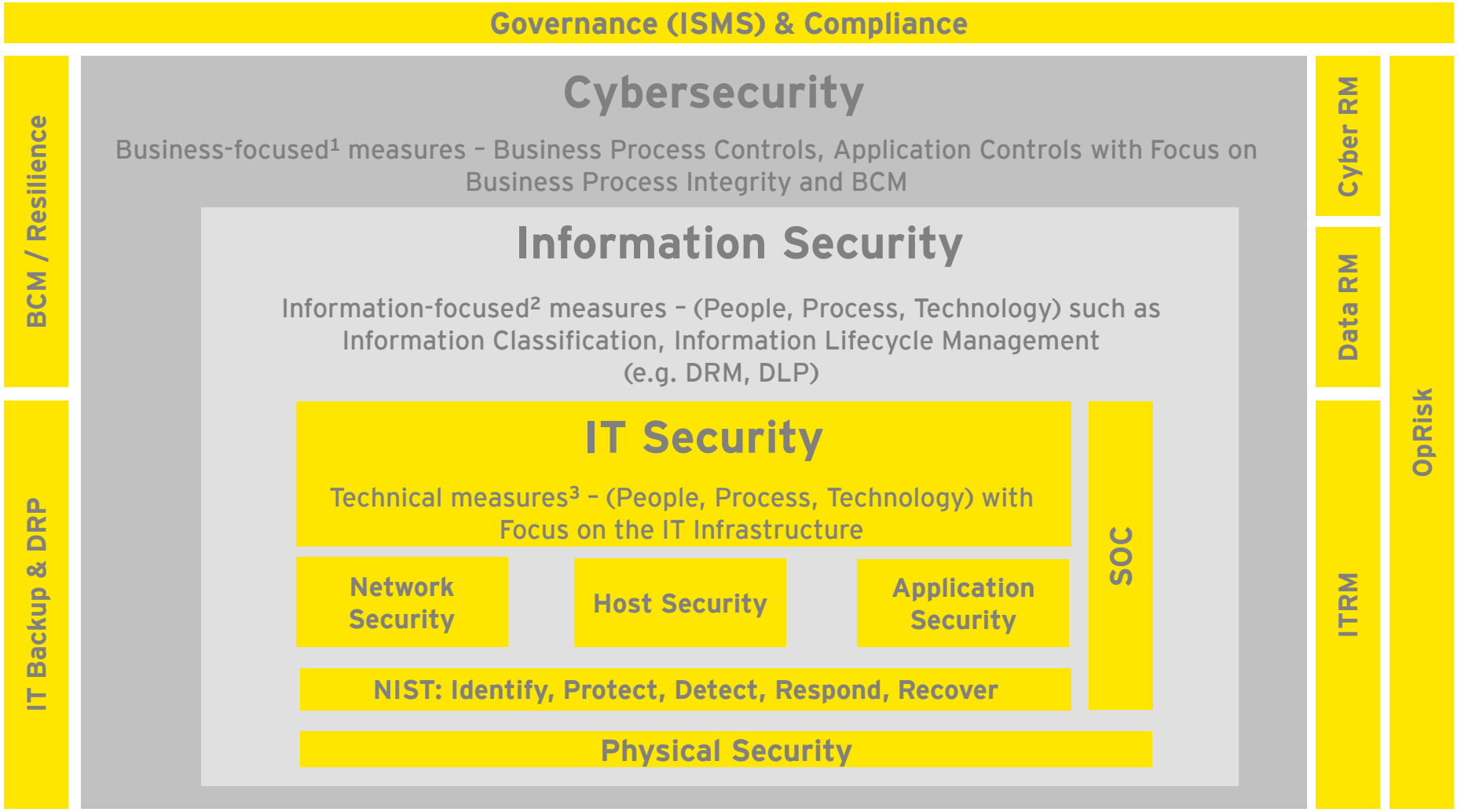


Cyber threats - Focus on cyber risks, not only on cybersecurity

Today's attackers have significant funding, are patient and sophisticated, and target vulnerabilities in people, process and technology.



Cybersecurity within your organization



1.) Business Centric 2.) Information Centric 3.) Technology Centric

01 Confront your cyber threats

EY's Global Information Security Survey

EY's 20th Global Information Security Survey (GISS) captures the responses of nearly 1'200 C-suite leaders and Information Security and IT executives/managers, representing most of the world's largest and most-recognized global organizations.

Responses were received from **59 countries** and across nearly all industries.

In **Switzerland**, we had **34 participants**, of which 20 stem from the financial services sector (banks, asset managers and insurance companies)

WWW For further information, please go to: ey.com/giss.

Confront your cyber threats

- All organizations are now digital by default, and need to operate with the cultures, technology and processes of the internet era.
- The integration and growth of the Internet of Things (IoT) is vastly increasing and complicating the networked landscape.
- Cyber attackers can be well-camouflaged: you need to be able to identify the threat even when it adopts the colors of its immediate environment.

The scale of the threat is expanding dramatically: by 2021, the global cost of cybersecurity breaches will reach US$6 trillion by some estimates, double the total for 2015.

Cybercrime Report 2017 Edition, Cybersecurity Ventures, 19 October 2017

While cybersecurity budgets are increasing, most organizations require more to manage the risk effectively

- Mounting threat levels require a more robust approach to cybersecurity.
- Most organizations continue to increase their spending on cybersecurity, though not all.
- The vast majority believe they need up to 50% more cybersecurity funding to enable the cybersecurity function to be in line with the existing risk tolerance of the organization.
- 76% of survey respondents said the cybersecurity budget would increase if they suffered a damaging breach.

59%
of respondents say their budgets increased over the last 12 months

87%
say they need up to 50% more funding to meet requirements

Only 12%
expect an increase of over 25% in their cybersecurity budget

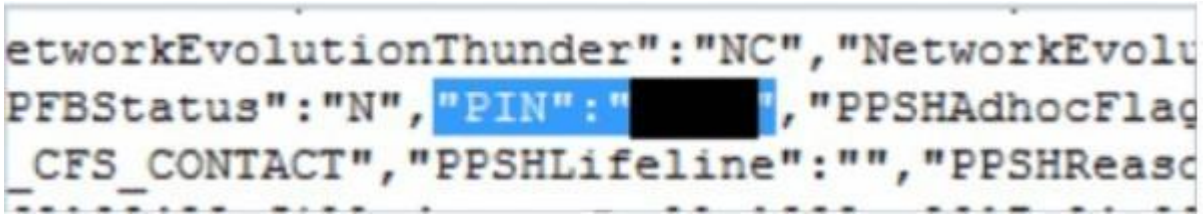
02 Examples to explain the current threat landscape

African Union hack / backdoor by Chinese Intelligence?

Russian nuclear supercomputer used for mining of crypto currencies

DNC hack: hacking like a fancy bear!

Cloud databreach on the rise



WannaCry: Costs that range in hundreds of millions

Ransomware in hospital: Medics say they couldn't wait for backups

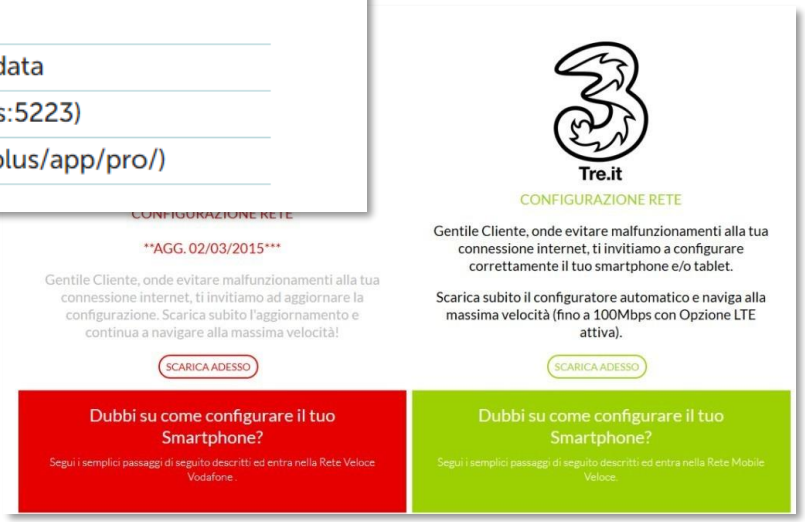
British cryptocurrency Electroneum hit by cyber attack after raising £30m

Hacking crypto currencies exchange platforms and coining malware

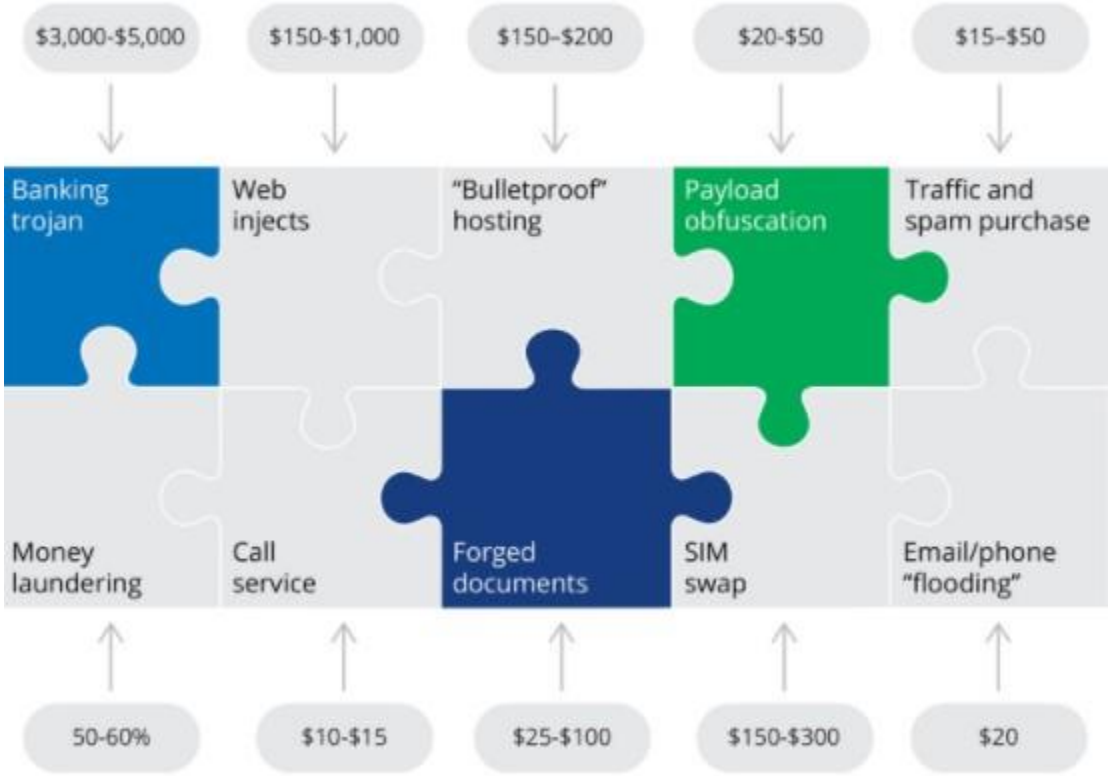
Huge data leaks

SkyGoFree spy tool

Service Name	Purpose
AndroidAlarmManager	Uploading last recorded .amr audio
AndroidSystemService	Audio recording
AndroidSystemQueues	Location tracking with movement detection
ClearSystems	GSM tracking (CID, LAC, PSC)
ClipService	Clipboard stealing
AndroidFileManager	Uploading all exfiltrated data
AndroidPush	XMPP C&C protocol (url.plus:5223)
RegistrationService	Registration on C&C via HTTP (url.plus/app/pro/)



Current darknet prices



Summary of current developments (1/2)
Continuity of trends which started in 2015 - 2017

- Increasing predominance of phishing and malware based attack
- Cybercrime in general is on the rise: target data sets are broadening (e.g. financial data, personal data, voter data, fraud)
- Crypto currency hack / mining
- 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 likely to be in focus going forward)
- Social engineering component of ransomware is becoming increasingly sophisticated (e.g. “infect two of your friends and get back your encrypted data for free”, malware kit is available for free to customers but provider asks for 30% of the customers’ victims)
- Developers will be increasingly targeted (backdoors in source code, compiler, development environment), hence this should also increasingly be in focus of audit functions
- Advanced and packaged hacking tools become more and more available to private companies (150k$) and not only reserved for governments
- Malware using more and more social media as C&C channel (e.g. Twitter, Google, etc.)

Summary of current developments (2/2)
New trends

Regulatory

- Increased government awareness, strengthening regulations (e.g. GDPR, penalties of up to 4% of worldwide turnover)
- Some regulators or actors moving to dual approach: top down (risk based) and bottom up (list of technical and specific controls)

Technologic trend

- Increasing value of crypto currencies: crypto-waterholing (NHS, US government court system, etc.), using nuclear classified super computers for crypto mining
- Governments and state agencies increasing support and control on private companies
- Collateral damage of weaponization of the cyber space by governments increases (e.g. Eternal Blue, NotPetya)

Key aspects to consider when addressing today's cyber risks

Back to basics

- Ensure solid and effective governance and basic defense capabilities
- In asymmetric warfare where attackers potential his higher than defense capabilities, defining the threat model is of paramount importance: identify what matters most, understand the threat landscape and define your risk appetite
- Keep working on the human factor: introduce or improve social engineering awareness campaigns
- Prepare for ransomware: patch, offline backup, monitoring and simulation

Shift focus from protection and prevention to detection and reaction

- Invest in meaningful threat intelligence (operational, tactical, strategic)
- Improve logging and monitoring of infrastructure and leverage a SOC solution for correlation

Maintain a holistic perception of security

- Keep an eye on regulators' requirements and implement accordingly if applicable to respective industry
- Keep thinking like an attacker: perform penetration testing/red team exercises and have an embedded hacker mindset in Cyber security programs
- Brace for vulnerabilities impacting security foundations such as standards/protocols or hardware by integrating them in your risk model and compensate with a layered approach of security

03 Understanding the threat landscape

Common, advanced and emerging threats and associated attack methods

The threat landscape

Common

These attacks exploit known vulnerabilities using freely available hacking tools, with little expertise required to be successful.

Advanced

Advanced attacks exploit complex and sometimes unknown (“zero-day”) vulnerabilities using sophisticated tools and methodologies.

Emerging

These attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities.

How to understand common threats/attacks

Description

Exploiting known vulnerabilities using freely available hacking tools, with little expertise required to be successful

Typical threat actors

Unsophisticated attackers, such as disgruntled insiders, business competitors, hacktivists and some organized crime groups

Examples

- Unpatched vulnerability on a website, exploited using a freely available exploit kit
- Generic malware delivered through a phishing campaign, enabling remote access to an endpoint
- Distributed denial of service (DDoS) attack for hire with a basic ransom demand

How to understand advanced threats/attacks

Description

Exploiting complex and sometimes unknown (“zero-day”) vulnerabilities using sophisticated tools and methodologies

Typical threat actors

Sophisticated attackers, such as organized crime groups, industrial espionage teams, cyber terrorists and nation states

Examples

- Spear phishing attacks using custom malware
- “Zero-day” vulnerabilities exploited using custom-built exploit code
- Rogue employees “planted” to undertake deep reconnaissance/ espionage
- Vendors/suppliers exploited as a way to gain access to ultimate target organization

How to understand emerging threats/attacks

Description

Focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities

Typical threat actors

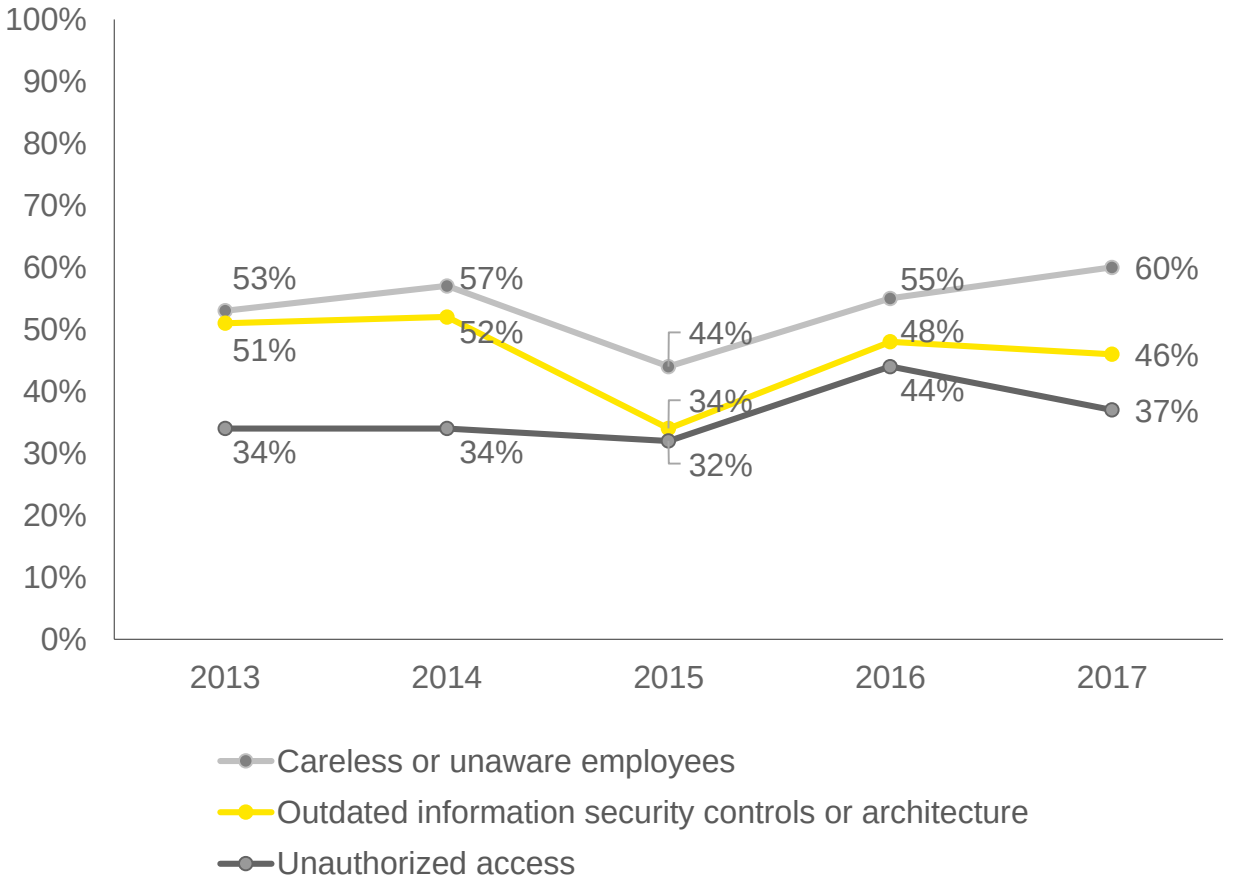
Sophisticated attackers, such as organized crime groups, industrial espionage teams, cyber terrorists and nation states

Examples

- Exploiting vulnerabilities on “smart” devices to gain access to data and/or control systems
- Leveraging security gaps created with the convergence of personal and corporate devices into one network
- Using advanced techniques to avoid detection and/or bypass defenses

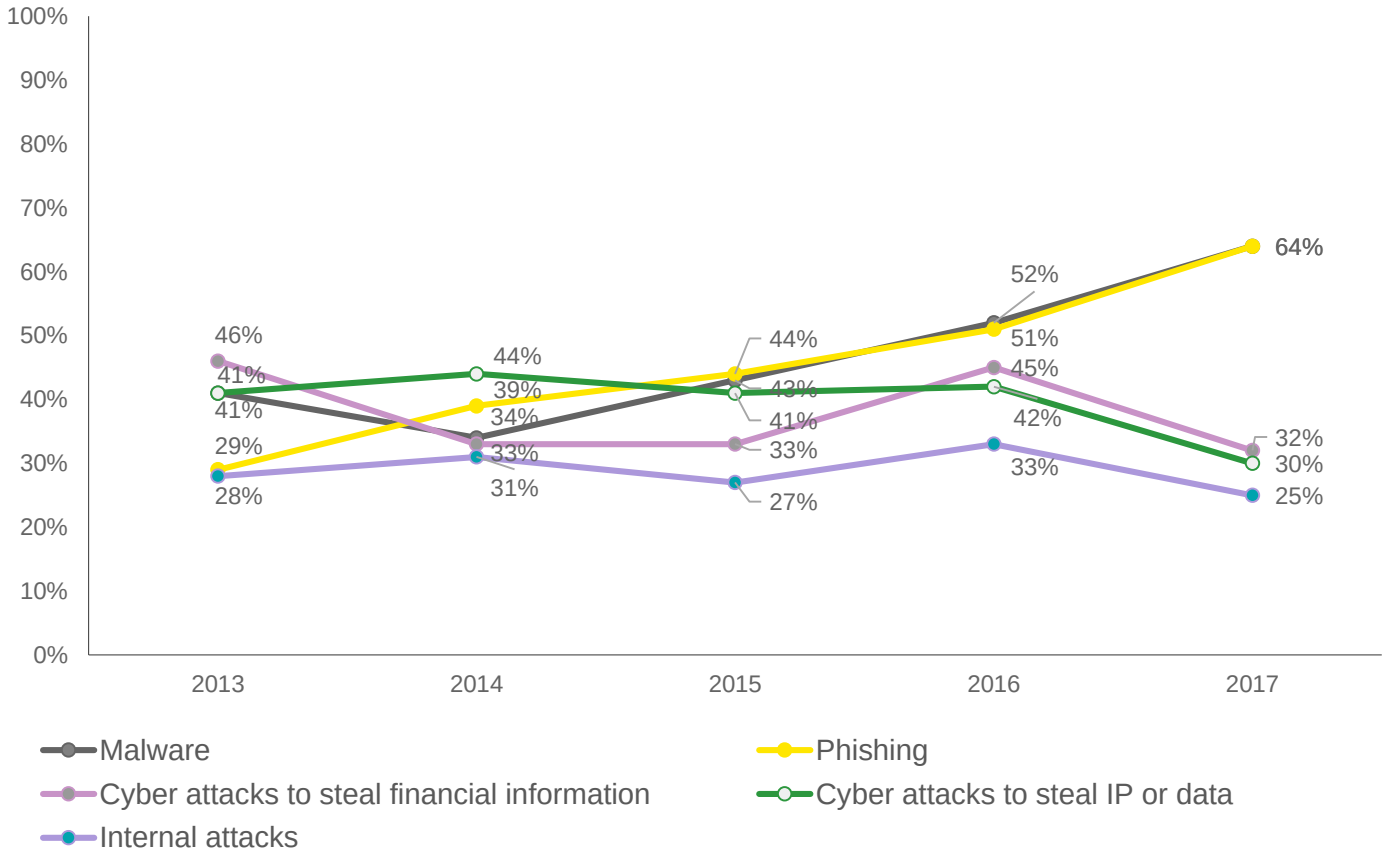
Vulnerabilities perceived to have most increased risk exposure have shifted a little between 2013-2017

- Careless or unaware employees are still seen as the greatest, and increasing, vulnerability.
- Unauthorized access has reduced as a vulnerability.



Threats perceived to have most increased risk exposure have shifted a little between 2013-2017

- Malware and phishing are seen as the greatest type of threats.



Likely sources of attack

- Employees and criminal syndicates are seen as the greatest immediate threats.
- For many organizations, the most obvious point of weakness will come from an employee who is careless – followed (in third place) by an employee with malicious intent.
- Organizations are also increasingly concerned about poor user awareness and behavior around mobile devices.

77%
of respondents consider a careless member of staff as the most likely source of attack

56%
consider a criminal syndicate as the most likely source of attack

47%
consider a malicious employee as the most likely source of attack

04 Conclusion

Conclusion

In previous editions of this survey, the need to structure cyber resilience has been highlighted around the principles of **protect, detect** and **react.**

- **Protect - basic hygiene makes an enormous difference**
- **Detect - as early as possible**
- **React - appropriately and swiftly**

These imperatives are more important than ever: organizations that understand the threat landscape and have strong defenses in place will stand a greater chance of repelling attacks, identifying successful attacks earlier, and responding effectively.

Those with the ability to fight back will limit the damage hackers can do by acting quickly.

Protect, detect and react should be applied to each category of threat/attacks:

- **Common**
- **Advanced**
- **Emerging**

To close, here are actions all organizations should take

Common attacks	Advanced attacks	Emerging attacks
Organizations need to be able to prevent common attacks through good basic cybersecurity.	Organizations need to focus on improving their ability to detect and respond to the more sophisticated and dangerous attacks.	Organizations need to understand the emerging threats and how they should impact strategic decision-making, while making focused investment in cybersecurity controls.
Example activities ▸ Establish effective governance ▸ Identify what matters most ▸ Understand the threats ▸ Define your risk appetite ▸ Focus on education and awareness ▸ Implement basic protections	**Example activities** ▸ Be able to detect an attack ▸ Be prepared to react ▸ Adopt a risk-based approach to resilience ▸ Implement additional automated protections ▸ Challenge and test regularly ▸ Create a cyber risk management life cycle	**Example activities** ▸ Build security into the development life cycle ▸ Enhance threat monitoring ▸ Establish Cyber Threat Intelligence capabilities

Questions?

05 Wrap-up, discussion and Appendix

References

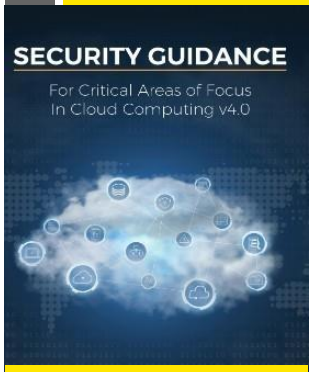
A SOC incl. SIEM & Cyber Sec. Analytics

MITRE

B Regulatorische und rechtliche Auflagen

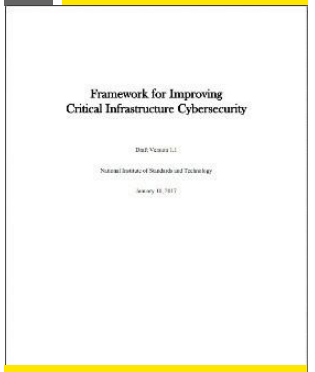
EY - SWIFT

C Cloud Security, Cloud Security Strategy



CSA

D1 Cybersecurity Strategie Review



NIST

D2 Cybersecurity Strategie Review

EY

D3 Cybersecurity Strategie Review

Center for Internet Sec.

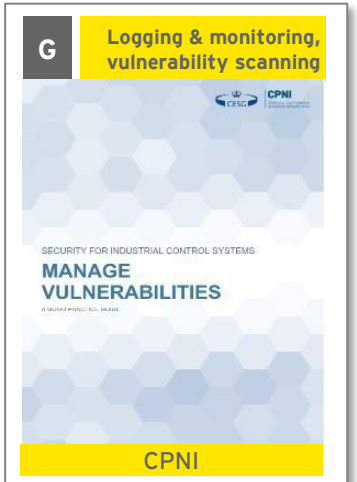
E IoT Cybersecurity

OWASP

F E- und M-Banking Fraud Detection

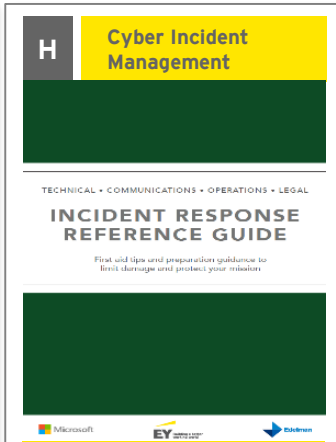
PCI

G Logging & monitoring, vulnerability scanning



CPNI

H Cyber Incident Management



MS / EY / Edelman

References

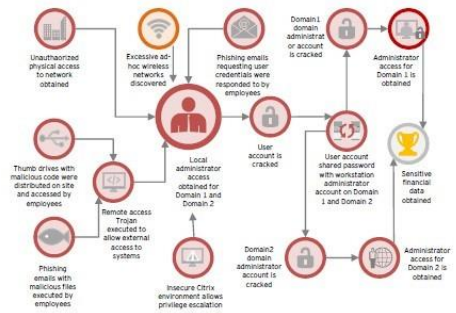
- A: MITRE: Ten Strategies of a World-Class Cybersecurity Operations Center
  https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf
- B: SWIFT: Customer Security Program (CSP):
  http://www.ey.com/Publication/vwLUAssets/ey-swift-customer-security-program/$FILE/ey-swift-customer-security-program.pdf
- C: CLOUD
  https://cloudsecurityalliance.org/guidance/#_overview
- D: NIST, EY (diverse Publikationen), Center for Internet security
  NIST: https://www.nist.gov/cyberframework - CIS: https://www.cisecurity.org/ - EY: http://www.ey.com/cybersecurity
- E: OWASP
  https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- F: PCI
  https://www.pcisecuritystandards.org/pci_security/
- G: CPNI
  https://www.cpni.gov.uk/cyber-security
- H: MS / EY / Edelman
  http://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf

Are you prepared to face the current cyber threat landscape?

49% of the responders of EY's 19th Global Information Security Survey (GISS) say that their organization is unlikely to be able to detect a sophisticated cyber attack.

Today companies are facing the challenge to adapt to the constantly changing threat landscape in a highly connected world. Organizations are no longer asking "are we secure", but "how can we ensure that the information most important to our business will be secure enough?"

EY's Red Team Assessment



The real world attack techniques used by EY are dynamic and based on which attack path testers determine is most likely to compromise the agreed upon target.

The end result is an attack-tree that demonstrates the different attack paths an adversary can use to capture the pre-defined trophies or targets.

This tree can for example combine external, social engineering, physical and wireless tactics to breach a company's perimeter security and is followed by internal testing tactics used to navigate the internal network and access the trophies.

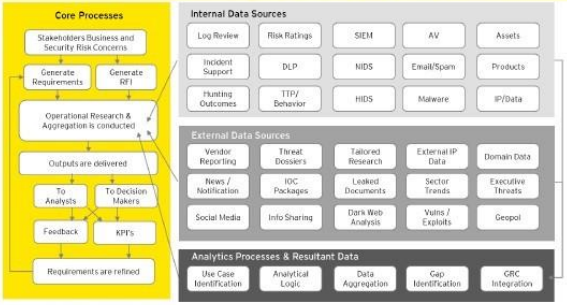
EY's Red Team Assessment is a threat intelligence based emulation of complex cyber attacks that mirror tactics of threat actors targeting your critical assets and business processes.

Red Team Assessments are intended to assess not only your resilience to real cyber attacks but also your team's (blue team) detection and response capabilities in a real world scenario.

57 % of the responders of EY's 20th Global Information Security Survey (GISS) do not have, or have an informal, threat intelligence program.

- Cyber Threat Intelligence (CTI) is about understanding cyber actors who might pose a threat to an organization.
- CTI is important in helping an organization decide appropriate controls and security posture. It is about "knowing your enemy".
- Buying intelligence feeds seems easy, but value is not realized if not properly integrated into the security stack.

EY's Cyber Threat Intelligence (CTI) Target Operating Model

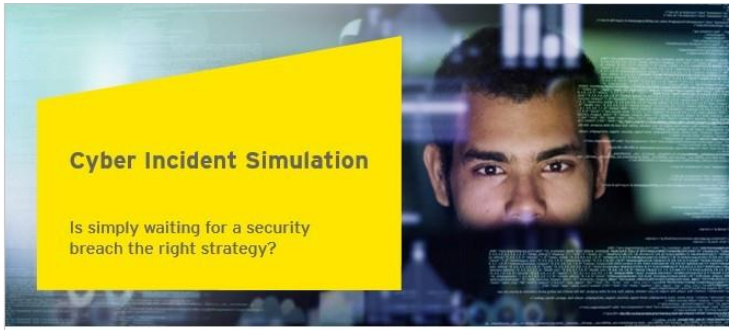


With the increasing number of CTI feeds and services, purchased threat intelligence is often too narrow in topic or overwhelming in quantity, and lacks insightful context. Security personnel and executive level decision-makers must implement and possess mature intelligence fusion methodologies and security capabilities in order to benefit from such services. A successful CTI program should implement a framework Target Operating Model to integrate the internal and external threat intelligence sources with the core processes of the organization using data analysis and analytics techniques. A cyber threat intelligence program is able to shed light on a multitude of strategic business concerns and risks while providing highly technical actions, countermeasures, and metrics to the cybersecurity program.

EY's CTI Target Operating Model provides a overall framework that ensures the interaction between various CTI elements to deliver actionable intelligence for both the security analyst and the key decision makers.

- How do you get better insights about tactics, techniques and procedures (TTPs) of current threat actors?
- Is your team/technology equipped to identify the threat early in the adversary life cycle?
- How can you take threat data and incorporate it into security operations and technologies to get ahead of the threat?
- How should you prioritize security solutions, countermeasures and resource planning based on CTI?

Is simply waiting for a security breach the right strategy?



Cyber attacks make headlines on a daily basis. It's no longer a question of if your organization will be breached, or even when, it's likely to have happened already. The real questions are: is your organization prepared to respond to a cyber incident?

57% of responders of EYs Global Information Security Survey (GISS) have had a recent significant cybersecurity incident.

Timeline of a possible cyber attack

Group CEO receives email from anonymous attacker	Sensitive customer data published on file-sharing website	Financial Times reporter receives calls the Group CEO to ask about the breach	A further 1,000 customer records are released	Group CEO receives another ransom email demanding payment of US$100m or all customer data globally will be released	Businesses in CH, SG, and HK cannot operate and deal with customer queries
Employees and IT teams arrive into work and can't login	Widespread speculation on social media and multiple media requests for comment/ statement	Regulator turns up at offices looking to speak to 'whomever is in charge'	Financial regulator in SG sends enforcement team to investigate	SG police investigators arrive at SG offices on foot of media reports surrounding extortion attempts	Law firm representing a small group of customers on a contingency basis threatens legal action to claim damages for data loss and fraud monitoring services

How would you respond:

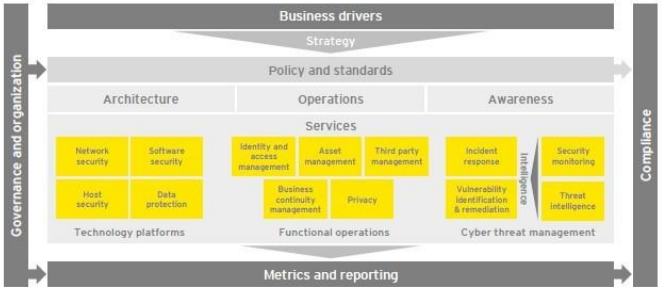
- Contacted by the regulator: What are your obligations?
- Compromised email systems: How do you communicate internally? Still via email, encrypted, WhatsApp or SMS?
- Media questions: What does your communication strategy look like?
- Compromised core application and loss of data integrity: Do you know for how long your system has been compromised? Can you rely on your backup?
- Ransom demand (Ransomware): Will you pay?

86% responders of EY's Global Information Security Survey (GISS) say that their cybersecurity function did not fully meet their organization's needs

Today companies are facing the challenge to adapt their business, to align their strategy and to be more efficient in a fast paced and highly competitive environment. The cyber threat landscape changes and presents new challenges every day.

EY's Cyber Program Assessment

Few companies today have the appropriate skills and resources in-house to effectively secure their information assets and at the same time optimize business performance. Therefore, EY's innovative Cyber Program Assessment (CPA) framework is built upon a meaningful analysis of how cybersecurity shapes and fits into an organization's overall risk management structure.



Even if your cyber team might be very well-equipped, it sometimes needs just a small flaw in the security posture to put the entire organization at risk: **How can you become aware of such deficiencies and the potential threat?**

Is risk still risky when you see it coming?

89%
say their cybersecurity function does not fully meet their organization's needs.

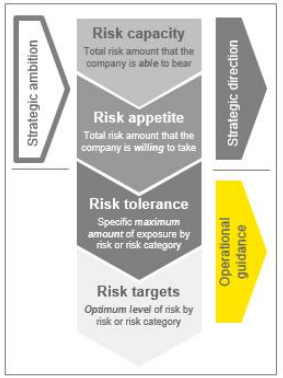
Is your Cybersecurity function managing risks within your corporate's risk capacity ? When done well, defining risk appetite establishes internal boundaries for prudent decision making, risk taking and highly efficient governance.

Managing Cyberrisk is a continuous process to keep the organization vital and protected from evolving attacks from the cyberspace

Enterprise risk managers (e.g. CRO) need to compare Cyberrisks to other risks using the same financial and probability benchmarks, so that investment on Cyberrisk prevention and remediation can be considered simultaneously with other pressing enterprise risks.

The board is expected to maintain oversight over the enterprise-wide Cyberrisk management strategy, including an appropriately set appetite for Cyberrisks, and to define the risk an organization is willing to assume within its risk capacity. It also has to validate that Cyberrisk management strategies and Cyberrisk appetites have been integrated into strategic plans and risk management structures in other areas of the enterprise.

Monitoring Cyberrisk should be done based on a defined set of Cyberrisk metrics indicating trends of an increased level of risk. However, specifying Cyberrisk appetite and Cyberrisk tolerance poses often challenges to an organization due to the unclear definition of the terms itself including the definition of Cyberrisk and Cybersecurity.



Why is risk appetite important?

Informs strategy
- A constant in an ever-changing environment
- Sets the boundaries for the firm
- A framework for evaluating opportunities

Makes risk culture tangible
- A mechanism for articulating and measuring the behaviors of the firm
- Underpins individual accountabilities

Cyber Insurance: the new product in the Insurance Sector and how EY can assist the Insurance Sector

Cyber Insurance is still relatively new in the Swiss Insurance market and its popularity is on the rise. In order for Insurance companies to provide insurance products and coverage, they need reliable historic data which will allow them to calculate their risk models. Furthermore, they require the right information in order to develop more competitive cyber insurance products for the market. As cyber threats have evolved, the need to assess a potential policy holder's cyber capability and to evaluate the cyber maturity have become increasingly important factors for insurance companies. When determining a corporation cyber insurance premium, these factors need to be taken into consideration.

EY can assist the Insurance Sector by offering a wide range of services to support the introduction and the operations of cyber insurance products by working closely with the Insurers, offering on-going cyber knowledge transfer, assessing cyber risk exposure of insurance clients as well as supporting the underwriting process of cyber insurance policies. Should a breach occur, EY can quickly support in the investigation as well as remediation of the breach, and therefore limit the damage caused and reduce the exposure.

How can EY support the Insurance Sector with the increasing and evolving need for Cyber Insurance?

1. **Cyber Security Knowledge Transfer**

   EY can offer its clients a cyber security knowledge transfer in the essential areas of prevention and proactive cyber threat detection and mitigation. Such an offering allows Insurers to successfully position themselves within the Swiss market with the Insurance Sector's latest product: Cyber Insurance.

   EY can work closely with the Insurer by offering their employees:
   - Up-to-date cyber training, cyber security best practices (including checklists);
   - Assessments and trainings relating to the latest cyber tools and methodologies.

2. **Cyber Risk Assessment**

   EY can assist the insurers, re-insurers, and underwriters with developing more competitive cyber insurance products. EY can perform a cyber risk assessment during the underwriting phase related to the acquisition of Cyber Insurance coverage and can assist with:
   - Understanding and evaluating their clients' risk exposure
   - Assessing the maturity of the current cybersecurity program as well as identifying areas for improvement
   - Validating that the security investments have improved their clients' security posture

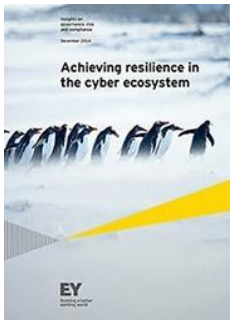
3. **Cyber Incident Response and Investigation**

   When a cyber attack has occurred, EY can assist the client with the investigation in order to quickly and efficiently close the breach, gather sufficient evidence of the breadth and depth of the compromise to enable successful remediation of the affected areas and immobilize the attackers. EY offers:
   - Global operational response capabilities
   - End-to-end services deployed within a mature forensic investigative framework
   - Advanced cyber analytics capabilities on big data platforms

Want to learn more? Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights

Cyber program management: identifying ways to get ahead of cybercrime

www.ey.com/CPM



Achieving resilience in the cyber ecosystem

www.ey.com/cyberecosystem

Cyber threat intelligence: how to get ahead of cybercrime

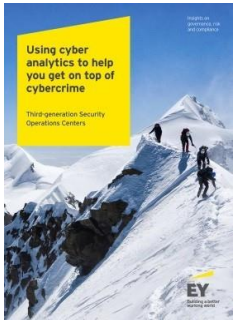
www.ey.com/CTI

Security Operations Centers - helping you get ahead of cybercrime

www.ey.com/SOC

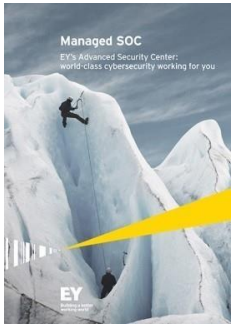
Using cyber analytics to help you get on top of cybercrime

www.ey.com/3SOC



Managed SOC EY's Advanced Security Center; world class cybersecurity working for you

www.ey.com/managedSOC

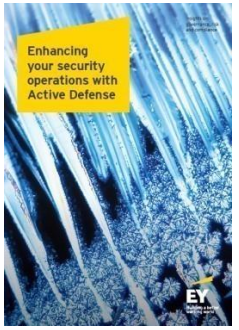


Cybersecurity and the Internet of Things

www.ey.com/IoT

Cyber breach response Management

http://www.ey.com/gl/en/services/advisory/ey-cybersecurity-cyber-breach-response-management



Enhancing your security operations with Active Defense

www.ey.com/cybersecurity

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Advisory Services
EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realize long-lasting results.

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

EYG no. 06575-173GBL

ED None

ey.com/giss

ey.com/ch