Protecting your business in a digital world

In our digitalized world, a week without new emerging events in the field of cybersecurity is very uncommon. Many organizations have already suffered cyber attacks or other security breaches. No organization can be 100% secure in today’s hyper-connected, borderless world. A cybersecurity breach can have devastating effects – from direct financial loss and decrease of shareholder value to reputational damage and liability exposure.

At EY, we recognize the importance of cybersecurity and have made it one of our top priorities. Our in-depth technical skills and extensive business knowledge enable us to determine the actual business impact. We have a proven track record in successfully advising C-level executives and board members on security strategy and transformation programs. As a trusted advisor at each organizational level, we support our clients in overcoming the challenges of protecting and securing their assets in a cost-effective way.

You can find a selection of our service offerings presented in this brochure. Let us work hand in hand to examine your cyber challenges, discuss specific aspects in greater depth and explore how our services could be applied to suit your needs.

“The question is not if your company will be breached, or even when. It has already happened. The real questions are: are you aware of it, and how well are you protected for the future?”

Tom Schmidt
EY Cybersecurity Leader Switzerland

Tom Schmidt
Partner, Cybersecurity Leader Switzerland
Creating trust in a digital world

The digital world abounds with rapidly expanding opportunities for innovation, and businesses, governments and individuals have turned their attention to the significant benefits. Digitization offers enormous potential — from creating new markets and products to finding innovative ways of connecting with increasingly knowledgeable customers.

Unfortunately, in the rush, many precautions have been overlooked and risks underestimated. The realization that there is a flip side, and that the digital world can also be exploited by criminals and others wanting to cause trouble, often comes too late.

In addition, complex, unintended consequences from the interconnectivity between people, organizations and “things” are starting to emerge.

For organizations to recognize the current challenges, and to understand what they need to do, they need to focus on each of the following four areas:

- Not enough measures in the current environment
- No mechanisms to adapt to change
- Slow proactive approach to neutralize sophisticated cyber attacks
- Why are you still so vulnerable?

The shift to Active Defense

- What is Active Defense?
- What needs to be improved?
- How to build Active Defense

- Today’s attacks on the digital world
  - How is the world changing for you?
  - What are the threats and vulnerabilities you should fear?
  - How can you manage the attacks?

- How attacks unfold
  - What are the worst case scenarios for you?
  - How to detect the small, subtle signs
  - Why “high alert” should be your constant state

- Why are you still so vulnerable?
  - Not enough measures in the current environment
  - No mechanisms to adapt to change
  - Slow proactive approach to neutralize sophisticated cyber attacks

Source: 18th EY Global Information Security Survey

57% of respondents say that lack of skilled resources is challenging Information Security’s contribution and value to the organization

59% see criminal syndicates as the most likely source of an attack today

88% of respondents do not believe their information security fully meets the organization’s needs

36% say it is unlikely they would be able to detect a sophisticated attack

88% of respondents do not believe their information security fully meets the organization’s needs

59% see criminal syndicates as the most likely source of an attack today

2 | Cybersecurity services  EY Financial Services Advisory 2016
In an increasingly interconnected world, the threat of cyber attacks is growing rapidly, and the impact of a successful attack can be devastating. A difficult balance needs to be struck between digital innovation and security controls.
Our value proposition

Trusted advisor

Our advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to provide a powerful and exceptional service. We use proven, integrated methodologies to support you in solving your most challenging business and cybersecurity challenges. With many years’ experience in cybersecurity assurance and advisory engagements, our cybersecurity team has a background in all aspects of digital security including penetration testing and incident response, threat intelligence management, security strategy and transformation.

Integrated perspective

EY is an acknowledged leader in the area of cybersecurity (Gartner, 2014 & 2015 and Forrester, 2013). At EY, we take an integrated perspective on all aspects of organizational risk. We understand the security challenge from a risk, regulatory, controls compliance and delivery perspective, leading our clients in end-to-end cybersecurity transformation. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

Global presence

Cybersecurity is a global issue that defies traditional boundaries – threats can impact your organization worldwide. Acting effectively is therefore crucial for organizations to minimize the impact of potential cyber attacks. EY’s global structure sets us apart from other professional services firms and enables us to transcend countries to deliver strong solutions at a global as well as a local level. Our organization is streamlined – it allows us to make decisions and investments quickly and ensures that we follow through with our strategy. No matter where in the world our clients do business, we can provide them with high-quality services.

“Our globally connected cyber professionals take an economical and geopolitical perspective towards cyber risk - giving a truer, fuller risk picture that aids strategic awareness and intelligent decision-making.”

Ken Allan
EY Global Leader, Cybersecurity

212,000 people, of which 39,500 in Advisory, serve clients across more than 150 countries worldwide and are specialized in various disciplines including cybersecurity
Organizations are still struggling to find the right response to the mounting cyber risks. In particular, they find it hard to align their security strategies with their real-world business strategies.

The best-prepared businesses now recognize that responsibility for deflecting cyber attacks can no longer be shunted off to their IT departments. Cybersecurity is a boardroom issue. The only sure way to counter the threat is using a strategic approach that roots your digital security in the real world of your business.

EY wants to support board members and C-level decision-makers in understanding the relationship between your responsibility and the scale of cyber threat. We offer a suggested approach that is sharply focused on your business structure, culture and risks.
Organizations are facing not only escalating risk, but also a high probability that they will suffer a cybersecurity breach in the future. A sharp focus on business structure, culture and risks will enable you to better safeguard the data essential to your organization's survival and success. This often requires a fundamental transformation in how cybersecurity is understood within the business.

Our Security Transformation services support organizations in tackling the many cybersecurity challenges they face on a daily basis and developing effective solutions. We leverage people, processes and technology to improve cybersecurity and risk decisions, reduce the costs related to managing cybersecurity risks and enhance our clients’ cybersecurity posture.

“Our Security Transformation services enable better security and risk decisions, reducing costs related to managing security risk and improving our clients’ information security posture.”

Services within Security Transformation

From time to time, it makes sense to review your existing security strategy – especially when introducing new services or implementing IT changes. With our Security Strategy and Roadmap services, we help you prepare for the future and leverage the benefits of IT and cybersecurity. Our approach is based on balancing risks and opportunities to provide you with recommendations tailored to meet your specific business needs. Beyond the strategy, we can assist you with evaluating and improving your organization's security.

Many organizations find it difficult to assess the impact of a cyber attack in real-world terms and understand how it can influence bottom line, brand and reputation. We assist organizations with analyzing business, financial and market data and cyber-economic information to deliver a threat intelligence-driven offering. By translating cyber attacks into tangible figures, we help you protect shareholder value, enhance ROI and respond to cyber-economic activities in good time.

Quantifying, classifying and measuring cybersecurity is a complex process. Our Cybersecurity Dashboard is a key tool in communicating the business value of cybersecurity to your various stakeholders. It provides top management with a high-level perspective on cybersecurity trends without losing focus of security operations. Together we can develop benchmarking, metrics and reporting that allow you to report on the performance of your security functions.

Our IT Risk Management services help transform risk, control and compliance environments. This is achieved by assessing, designing and implementing solutions around process risk and controls that enable technologies to support their efficiency and effectiveness. We help leverage and improve IT risk management programs through current-state assessment; IT process, risk and control (PRC) framework design; development and implementation support; and support of methodologies and procedures.
Our Cyber Program Management (CPM) services enable organizations to draw on their various resources to tackle the many security challenges they face on a daily basis. Any organization stands to benefit from an objective assessment of its cybersecurity posture and related programs that assists with:

- Understanding your organization’s risk exposure
- Assessing the maturity of your current cybersecurity posture and identifying areas for improvement
- Building a prioritized road map for project investments and organizational change initiatives
- Collecting information to create benchmarks against other organizations
- Determining whether your security investments have improved your security posture

Such an assessment needs to be broad and high-level as well as completely embedded in specific areas and components. EY can work hand in hand with you to identify what is needed to support the ongoing assessment, transformation and sustainability of your cybersecurity strategy.

EY’s current-state maturity benchmarking tool (example case study)
Considering today’s cybersecurity landscape, it is no longer possible to prevent all attacks or breaches. In a corporate context, a cyber attack can not only damage your brand and reputation, it can also lead to legal/regulatory non-compliance, steep financial damage and a loss of your competitive advantage.

Our Cyber Threat Management services support organizations with detecting and responding to these real-world threats in the context of their own business, improving their overall cybersecurity posture. In addition, relevant, timely and accurate information is critical for an organization to achieve effective operations within any Cyber Threat Management program. By bringing together and establishing the right sets of data that will support advanced analytics, we enable the delivery of value-added services that reduce risk, address incidents and enable decision-making.

“Our broad range of Cyber Threat Management services provides you with the means to protect against, detect and respond to rapidly evolving cyber threats.”

Services within Cyber Threat Management

Our global Attack & Penetration testing methodologies reflect the latest approaches at network, service and application levels. Our approach emphasizes end-to-end verification of the risk and business impact of individual findings as well as vulnerability linkage. To also address the response capabilities within the organization under review, we perform “red teaming” activities (goal-based penetration testing, where internal IT staff must identify and stop an attack with limited advance information).

With the “Am I compromised” assessment service, we help organizations understand the cyber risks they are facing. By assessing real-time network traffic, we search for indicators of compromise using advanced malware detection tools. We determine the impact on the business through scenario-based assessments. The results can be used to assess and enhance the control environment.

By analyzing security logs, transaction data, network logs and behavioral information, we provide insights into real threats that have an impact on the business. This enables an organization to identify and mitigate threats as well as to respond quickly and effectively.

The key part of getting ahead of cybercrime is having the right response to a potential cyber attack or data breach. With our Cyber War Games, we provide organizations with a rapid, independent assessment of their current capability to detect and react to the broad range of cybersecurity threats based on a cyber incident response scenario. The results of the Cyber War Games are used to help organizations mature in their cyber response capabilities.
In the upcoming years, a shift will occur in identity provisioning. Smart meters, connected cars and smart watches will become integrated into the digital world. This drastically changes the number of identities organizations have to deal with. It changes authentication. It requires management of relationships between identities and massively expands the scope of identity and access management, which has to become risk-based and — with the ever-changing scope — dynamic. Identity and access management is a key element in enabling the use of technologies and achieving business objectives, further emphasizing the need for it to grow beyond a mere compliance solution into a valued business tool.

Our services are focused on business enablement and provide you with the ability to identify opportunities to continuously and efficiently manage system access and mitigate risks in relation to confidentiality, integrity and availability of critical data.

"Our Identity and Access Management service portfolio enables you to manage your organization’s access to resources and identities."

Services within Identity and Access Management

IAM Strategy, Roadmap and Implementation

We work with you to advance your IAM strategy, including support in the development of an IAM operating model and governance structure, IAM policies, procedures and standards assistance, IAM program management assistance, IAM compliance, privileged access management, roles and rules management and segregation of duties (SOD) management programs.

IAM Diagnostic and Intelligence

This service complements Strategy, Roadmap and Implementation, covering both internal and external identities, and includes assisting with current-state assessments, capability maturity and benchmarking assessments. IAM diagnostic assessment also comprises IAM data analytics, application access assessments and IAM business performance. IAM business performance includes assisting organizations with defining and implementing IAM monitoring and reporting, IAM metrics as well as KPIs and SLAs.

Role and Digital Identity Management

As an organization grows, the roles within it become more diverse and access profiles widen. We help organizations mitigate their IAM risk by analyzing which roles are vital to the organization and determining how these roles should be as well as searching for toxic combinations. Our services also help organizations to establish common technologies and processes to manage identities and access with partners and third parties. These processes include consumer and citizen identity data management.

IAM Access Review

This service involves establishing business-friendly internal and external identity access review processes, guidelines and procedures that: (a) route review tasks to parties who are familiar with the access needs of the users subject to access certification, (b) identify potential segregation of duty (SOD) conflicts in reports designed to support certification and (c) support periodic certification of roles, rules and entitlement definitions and ownership.
The rising costs and increased media coverage of data breaches and the continued escalation of threats facing organizations have led to cybersecurity, particularly data protection, being discussed at the highest level.

Our Data Protection & Privacy professionals can help assess, design and implement the processes and technology required to build a sustainable data protection/privacy program that is aligned with your business needs and focused on protecting the data that matters most. We can draw on many years of delivering services in implementing and consulting on data protection programs to clients around the world. Tapping into this expertise enables you to realize better value from your investments.

**Services within Data Protection & Privacy**

- **Data Protection Program Transformation**
  - Our data protection professionals help you develop and implement your organization’s data protection program, focusing controls on the data that matters most. These controls link to the numerous information security processes, which must be effective to support the confidentiality, integrity and availability of data. By assessing current data protection program governance model, data-at-rest, data-in-motion and data-in-use processes and controls to identify gaps, we help establish maturity goals and the initiatives needed to achieve them.

- **Data Loss Prevention Assessment**
  - This service uses data loss prevention (DLP) technology to assess the risks of data loss or leakage in a client’s environment. Such an assessment includes using specific DLP software deployed by EY in the client’s environment to help identify sensitive data stored in file repositories and sensitive data leaving the client’s environment through email and/or online communication.

- **Data Privacy**
  - Our Data Privacy service assists organizations with assessing, developing and implementing privacy programs. This may include mapping data flows of personal information, evaluating processes and controls in place for the collection, transmission, usage, storage and protection of personal information, and identifying and helping to remediate gaps in the privacy program using generally accepted privacy principles or other specific industry, national and state regulatory requirements.

- **Data Protection Audit and Impact Assessment**
  - Working alongside leading experts from EY’s Legal, Regulatory & Compliance practice, we ensure that organizations remain compliant with applicable laws and regulations (e.g., EU General Data Protection Regulation). By conducting data protection audits and impact assessments, we can help you identify and remediate compliance gaps across the organization.

“This suite of services puts you in a position to build a sustainable data protection and privacy program that is aligned with your business needs and focused on protecting the data that matters most.”
Consumer demands, disruptive technology and the call for clear visibility across the enterprise have organizations struggling to keep abreast of rapidly changing cybersecurity needs. Some have limited resources qualified to navigate an increasingly demanding environment. Others find that the complexity of their cybersecurity solution has increased costs and hampered agility.

Our Managed Cybersecurity Services offer organizations state-of-the-art technology, knowledgeable professionals, flexibility and scalability to address today's business challenges – for a significantly reduced and more predictable cost than doing it in-house. By choosing our services, you can let us worry about the risks associated with e.g., vulnerability management, security monitoring and incident response, allowing you to get on with the business of driving growth and accelerating performance. The EY Advanced Security Centers (ASC) offer sophisticated technical facilities and a staff of dedicated security professionals who are ready to assist our clients 24/7/365. Our globally integrated laboratory centers are based in Argentina, Australia, India, Ireland, Israel, Malta, Philippines, Singapore, Spain and US.

Services within Managed Cybersecurity Services

Vulnerability Identification
Vulnerability Identification goes beyond Attack & Penetration Testing services and includes periodic scans of an organization's network infrastructure and systems as well as applications and source code reviews using best-in-class tools. We support organizations in identifying the appropriate remediation and support them with escalating technical issues.

Managed Security Operations Center (SOC)
The Managed SOC service emphasizes security monitoring and incident response. This includes monitoring infrastructure, threat and alerts intelligence/analysis and up to 24/7/365 monitoring to identify known malicious or suspicious traffic entering or exiting your network, or attackers moving laterally, escalating privileges and stealing data from your environment. Following the identification of malicious activity, the incident response team assesses the nature of the attack and defines and implements the most appropriate response.

Cyber Threat Intelligence
Our managed Cyber Threat Intelligence services combine various aspects of security operations. We can map out the threat landscape and put historical data into context. As our Cyber Threat Intelligence program matures, predictive capabilities are uncovered, allowing management to make decisions that are based on historical precedent rather than intuition.
Cybersecurity should not be viewed as an obstacle, but as a means of fully and sustainably tapping into the digital world.

Cybersecurity is key to unlocking innovation and expansion. By adopting a bespoke and risk-centric approach to cybersecurity, organizations can refocus on exploring business opportunities. Building trust in a business that operates successfully within the Internet of Things (IoT) and that fully supports and protects individuals and their personal devices – from simple smartphones to health care devices and smart cars – is a key competitive differentiator and must be a priority.

You can adjust the balance of the digital world back toward sustainability and safety. Acting now allows you to better protect your organization and create trust in your brand.
Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These up-to-date and topical publications are designed to help you understand burning issues and provide you with valuable insights into our perspective.
Contacts

Tom Schmidt
Cybersecurity Leader Switzerland
Phone: +41 58 289 64 77
Email: tom.schmidt@ch.ey.com

Reto Aeberhardt
Cyber Program Management (CPM) and Security Transformation
Phone: +41 58 289 67 40
Email: reto.aeberhardt@ch.ey.com

Stefan Wenigmann
Cyber Threat Management and Managed Cybersecurity Services
Phone: +41 58 289 67 56
Email: stefan.wenigmann@ch.ey.com

Adrian Rogg
Identity and Access Management and Data Protection & Privacy
Phone: +41 58 289 35 99
Email: adrian.rogg@ch.ey.com
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.

© 2016
Ernst & Young Ltd
All Rights Reserved.

ED None

This publication contains information in summary form and is therefore intended for general guidance only. Although prepared with utmost care this publication is not intended to be a substitute for detailed research or professional advice. Therefore, by reading this publication, you agree that no liability for correctness, completeness and/or currentness will be assumed. It is solely the responsibility of the readers to decide whether and in what form the information made available is relevant for their purposes. Neither Ernst & Young Ltd nor any other member of the global EY organization accepts any responsibility. On any specific matter, reference should be made to the appropriate advisor.

www.ey.com/ch