Is the answer to cybersecurity more technology, more people or more process?

Cybersecurity can only be addressed by combining technology and business acumen with unique human insights.

ey.com/betterworkingworld #BetterQuestions

The better the question. The better the answer. The better the world works.
“EY Cyber's mission is to build a more secure and trusted working world.”

Cybersecurity is not just a technology or risk issue. It’s a strategic business imperative. That’s why we bring a cross-functional team of cybersecurity professionals, business advisors, investigators, and technical and IT risk practitioners to help you tackle your biggest challenges.

With digital and geopolitical threats increasing, businesses need more than an off-the-shelf security solution or basic risk mitigation to protect critical assets. These threats expose the real reputational and financial risks your organization faces.

Ernst & Young LLP has invested heavily in infrastructure, technology and talent to help you operate your business, and capitalize on opportunities while under attack and manage your risk profile. Our Cyber practice unites talents from both the public and private sector, including the National Security Agency (NSA), the Central Intelligence Agency (CIA), the US Air Force, the US Marines, the Federal Bureau of Investigation (FBI) and leading technology companies all over the world.

To thrive, you need the ability to adapt. That means embedding cybersecurity resilience everywhere – at every level of your organization. It’s the intersection of business strategy, risk management, digital evolution, real-time operations, technology innovation and predictive analytics that allows you to prioritize the right decisions, faster! Having experience in your industry allows us to understand the specific challenges you face in protecting your business. Our global ecosystem of talent, strategic alliances, intellectual property, managed services and technologies means we bring the right insight at the right time. While complexity increases every day, we continue to collaborate with you to give your organization real-time agility and resilience against cybersecurity threats while enabling growth and opportunity.
Our cyber capabilities

Digital and Analytics
- Security Analytics Services
  - Data, Identity, Behavioral and Cogitative
- Internet of Connected Things Security Services
  - Operational Technology Security
  - Internet of Things (IoT) Security Services
- Cloud and Mobility Security Services
  - Digital Trust
- Data Identification and Protection Services
- Social Media Security Services
- Digital Identity Security Services

Defense and Response
- Threat Detection and Response Management Services
  - Incident Response
  - Threat Intelligence
  - Active Defense (Hunting)
  - Red Team Services
  - Security Operations Services
- Threat Exposure Management Services
  - Software Security Service
  - Product Security Services
  - Vulnerability Identification and Management

Strategy and Architecture
- Architecture and Design Services
  - Identity, Data, Threat
- Strategic Assessment and Program Services
  - Countermeasure Assessment
  - Technology Strategy Assessment
  - Strategic Intelligence Program
- Business Risk Strategy
- Analytics Strategy
- Operations Strategy
- Identity Strategy

Cyber Operations
- Cyber-as-a-Service Offerings
  - Threat Detection and Response Monitoring Services
  - Security Operations Monitoring Service
  - Insider Threat Monitoring Service
  - Cloud Security Monitoring Service
- Threat Exposure Monitoring Services
  - Software Security Monitoring and Protection Services
  - Vulnerability Identification Scanning and Protection Service
  - Internet of Connected Things Monitoring and Protection Services
- Data Identification, Protection and Monitoring Services
- Identity and Access Monitoring Services

Governance and Compliance
- Cyber Regulations, Privacy and Compliance Services
  - Program Development and Improvement
  - Assessments Services
- Cyber Governance and Policy Services
  - Identity and Privileged
- Regulatory Inventory and Data Classification Services
- Privacy Assurance

Technology and Innovation
- Cyber Innovation
  - Insider Threat Identification Service
  - Medical Device Vulnerability Identification Service
- Autonomous Car Vulnerability Identification Services
- Cyber Orchestration and Robotics Services
- Advanced Malware Detonation Services
- Cyber Technology Ecosystem
  - Microsoft Security Services
  - IBM Security Services
  - SAP Security Services
  - GE Digital Security Services
  - Cisco Security Services
- Advanced Technology Implementation Security Services
Digital is poised to redefine the human-to-business experience. Digital solutions are creating new economies, new communities, new processes – a new normal expectation. Designed to eliminate corporate boundaries by embracing analytics and machine learning, mobile, cloud, and the Internet of Connected Things, digital solutions have the ability to predict, detect and respond to needs without conscious intervention.

**Data identification and protection**
Securing data throughout the digital experience is critical to achieving the expected value. Evaluating existing applications and deploying new ones that detect, prevent and report suspicious activities can help manage the risk associated with digital data.

**Digital identity and access**
Next-gen identity and access management accelerates productivity, improves end-user digital experience and decreases cost of ownership. Anyone, anywhere, any device, anytime.

**Software and product security**
Enabling security throughout the software development life cycle.

**Analytics**
Modeling and deploying descriptive, diagnostic and predictive analytics provide insights in real time to detect and respond to digital risks.

**Cloud and mobility**
Secure solutions throughout the life cycle include readiness evaluations, secure design, development, governance and transition to operations.

**Internet of Connected Things (ICT)**
From connected devices to embedded sensors, our ICT services identify vulnerabilities and risks; support the design and development of secure solutions; and provide comprehensive digital security operation center support.

The digital transformation of IT and business into new markets like cloud, mobile, ICT and social media has opened new security weaknesses in your environment.

**How can you identify and manage the risk associated with your digital strategy?**

**Analytics**
- Advanced cybersecurity analytics will help your organization develop predictive capabilities and give you visibility into the dark spaces of your network.

**Cloud and mobility**
- As the digital transformation continues to accelerate, cloud and mobile adoption is the first platform to be leveraged.
- How are you maintaining security over these platforms?

**Internet of Connected Things**
- Computing hardware gets smaller, and every device becomes connected.
- How are you maintaining your security posture during this type of adoption?

**Social media**
- Social media is being leveraged by more organizations every day and by more malicious actors every day.
- How do you protect your data over these platforms?

**Digital identity and access management**
- The organization becomes compromised, and malicious actors steal your credentials.
- How do you manage and protect your credentials over the cloud?

**Data identification and protection**
- Organizations continue to leverage and expand their data repositories.
- How are you maintaining security awareness and protection of all your critical data?
Cyber Defense and Response services delivered through advanced security centers (ASCs) help clients thwart, detect and respond to real-world attacks and improve their overall cybersecurity posture.

Cyber Defense and Response

Building trust
Our vision is that the initiation and integration of the components of our framework provide our clients with relevant and actionable insight.

Time to fix
These services can be delivered through a traditional advisory approach or as a managed service offering through Cyber-as-a-Service.

How can you prevent, detect and respond in minutes?

- **Cyber threat intelligence**
  > Cyber threat intelligence informs decision-makers and security teams by quantifying and qualifying threats in cyberspace.

- **Security monitoring**
  > Detect and respond to attacks before critical company services are disrupted or high-value assets are compromised.

- **Incident response**
  > Prepare for the inevitable attack and manage the aftermath of an incident or data breach.

- **Vulnerability management**
  > Identify and manage security vulnerabilities across deployed technologies for timely remediation.

- **Vulnerability identification**
  > Provide a simulated test and help assess the extent to which the organization is vulnerable.

- **Software security**
  > Proactively identify and remediate security vulnerabilities during the software development life cycle.
Cybersecurity is a top risk for companies, but it’s too often addressed tactically and reactively. Our Cyber Strategy and Risk services allow our clients to build a strategy and cyber function that is aligned with their business objectives. It is data-driven and provides a sustainable and defensible cyber capability.

- Spending needs to be aligned to mitigate the risks that matter most.
- We provide peer comparison benchmarking and analytics-driven decision support for where the next incremental dollar should be spent to maximize impact.
- Our clients should be focused on taking risks to grow their business via new products and markets without undue focus on cyber.
- We codevelop strategies and organizations to empower business growth by mitigating risks that could disrupt the achievement of business goals.
- Our focus on data-driven analytics provides our clients with real-time performance management capabilities via dashboarding and continuous monitoring.
- Management and the board can understand how their investments in cyber are producing real risk reduction.

How do you scale and increase security situational awareness with limited people?

- **Program assessment**
  - Evaluating the current capability of the cyber function through analytics and process maturity
- **Strategy and road map development**
  - Defining the cyber function’s ability to appropriately and sustainably protect business and information assets
- **Program co-sourcing and transformation**
  - Providing services and surge staffing support to effect a sustainable cyber program transformation
- **Program analytics and executive reporting**
  - Enable data-driven continuous monitoring of the cyber function and its ability to meet changing business and threat conditions
Cyber Defense and Response services delivered through advanced security centers (ASCs) help clients thwart, detect and respond to real-world attacks and improve their overall cybersecurity posture.

**Speed to maturity**
Ability to move your program up the maturity curve rapidly with proven methodologies, processes and technology

**Lower start-up costs**
No need for you to invest significant staff and up-front capital to increase maturity and capabilities

**Scalable service**
Meets changing resource bandwidth requirements without locking in full-time resources, leveraging economies of scale where practical

**Access to specific, scarce skill sets**
Resources offer sector-specific knowledge and multidisciplinary experience

**Access to global resources**
Facilitates localized knowledge (languages, geographies)

**Freed-up resources**
Facilitates resource redeployment to focus on other value-added activities to manage your business

**Proven tools and methodologies**
Enables repeatable and efficient security management activities

---

How do you scale and increase security situational awareness with limited people?

**Threat Detection and Response**
- Threats are identified and remediated before high-value assets are affected.
  - Automated detection lowers incident investigation costs.

**Threat Exposure Management**
- Proactively discovers and remediates vulnerabilities.
  - Ninety-nine percent of exploits are through vulnerabilities that have been published for over a year.
  - This service reduces the likelihood of an exploit and mitigates the risk of a cyber breach.

**Identity and Access Management**
- Promotes controlled access to resources.
  - User provisioning is automated.
  - Spending becomes more predictable.
  - Cost of ownership is lowered.

**Data Protection**
- Guards critical and sensitive data.
  - Round-the-clock data loss monitoring and response capabilities protect against a breach.
Cyber-related regulatory and compliance requirements are expanding well beyond industry-specific mandates.

**Assessment Services**
Provide management with insights into the maturity of its programs and approaches for transforming identified areas of concern.

**Remediation Services**
Help the entity address areas of concern with its program and help the entity better understand: (1) the type of information accumulated, (2) the flow of the information throughout the entity, (3) the processing of information and (4) the adequacy of controls over information retained on its systems.

**Implementation Services**
Assist the entity in defining and standing up programs that are responsive to its regulatory and compliance requirements.

**Reporting Services**
Communicate the entity’s level of compliance to interested parties’ assurance management activities.

---

**How do you scale and increase security situational awareness with limited people?**

- **Program assessment**
  - Evaluating the current capability of the cyber function through analytics and process maturity

- **Personal Information Inventory and Data Flow**
  - Personal Information Inventory
  - Personal Information Flow Documentation

- **Privacy Program Development and Improvement**
  - Program Strategy and Development
  - Policy Development
  - Compliance and Monitoring

- **Privacy Assurance**
  - Privacy SOC 2/3
  - Other attestation reports

---

* GDPR = Global Data Privacy Regulation | CBPR = Cross Border Privacy Rules | FISMA = Federal Information Systems Management Act
EY Cyber continues to develop and work with the most cutting-edge and innovative companies in the cyber ecosystem to bring a new level of experience and provide innovative offerings to our clients.
Why EY Cybersecurity

- **Trusted and knowledgeable** | Fusing strategy, financial, risk and operations in your business

- **Business and technical advisors** | Translating cybersecurity into your business language and aligning it with your business strategy

- **Industry-focused experience** | Possessing deep Industry knowledge and experience

- **Broad global perspective** | Bringing insights across all business lines

- **Connected and scalable** | Benefiting from an ecosystem of cybersecurity talent, local to your global teams

EY is well-known for employing a diverse and deep bench of cyber talent. We've brought in highly experienced professionals from some of the largest technology companies in the world and paired them with executives from the most pioneering technology start-ups. We combine that with leaders who have served in the public sector through the FBI, the CIA, Homeland Security, and the US Army, Air Force and Marines. Our ecosystem of talent allows us to bring broad perspective, deep experience and innovative strategies.
Areas of focus

cybersecurity, military, law enforcement, government, industry, technology

- risk management
- strategy
- boards
- compliance
- implementation
- advanced protection
- forensics
- digital
- threat intelligence
- DLP
- incident response
- analytics
- red teaming
- privacy
- maturity
- data
- operations
- active defense
- transformation
- software security
- innovations
- vulnerability management
EY Cybersecurity size and scale

Number of countries: 150
Cybersecurity practitioners globally: 7,000
Gartner-rated cybersecurity leader: #2
Cybersecurity Ventures: #1

"Gartner, Inc. has ranked EY second in worldwide market share in the information security consulting market, based on total revenue for 2015."

“Today’s threat landscape is ever-changing and requires our vigilance and resilience. That is why EY remains committed to building a more secure working world by investing in our leading-class cyber practice.”

– Barbara O’Neill
EY Global Chief Information Security Officer
A vibrant alliances ecosystem

Alliance relationships are at the heart of EY’s ability to address the most relevant and significant issues our clients face today including cybersecurity. For example, our relationship with Los Alamos National Laboratory delivers some of the most advanced behavioral cybersecurity tools available to the commercial market.
“At EY, we understand the challenges that our clients face, and we are always looking for new innovative ways to leverage technology to drive a new result to a difficult challenge.”

— EY Strategy, Innovation and Growth Leader

Cyber innovation

Every day, EY Cyber is working to help our clients solve some of their largest challenges. Whether it’s maximizing their cyber investment, building technology to aid automation or creating new methodologies for securing emerging technology such as autonomous cars, EY is here to help.

How do you transform to address the digital market without losing your security posture?

How do you continue to innovate and stretch toward what is possible?

How do you build robotics around your ecosystem of security vendors?

How do I maximize throughput, quality and total cost?

EY Cyber can help with business models and experiences; develop and co-create concepts; pilot ideas at a small scale; and research and fashion technologies and techniques that drive the future of cybersecurity.

Sustainable Cyber innovation

Autonomous cars

Medical devices

Virtual and augmented reality

Automation and robotics
We’re not only accountants. We’re trusted advisors who understand how cybersecurity risks can impact your financials and your organization. Having business advisors, integrators, operators and strategists on staff, we can help you build cyber awareness and resilience at every level of your organization. As technology and cyber professionals adept at both IT infrastructure and digital trends, we are the ones to help you ask – and answer – the better questions needed to capitalize on your business opportunities while negotiating the threat landscape.

Americas Cybersecurity Leader

Bob Sydow
bob.sydow@ey.com