Path to cyber resilience: Sense, resist, react

A presentation of results from the industry:

Industrial Sector

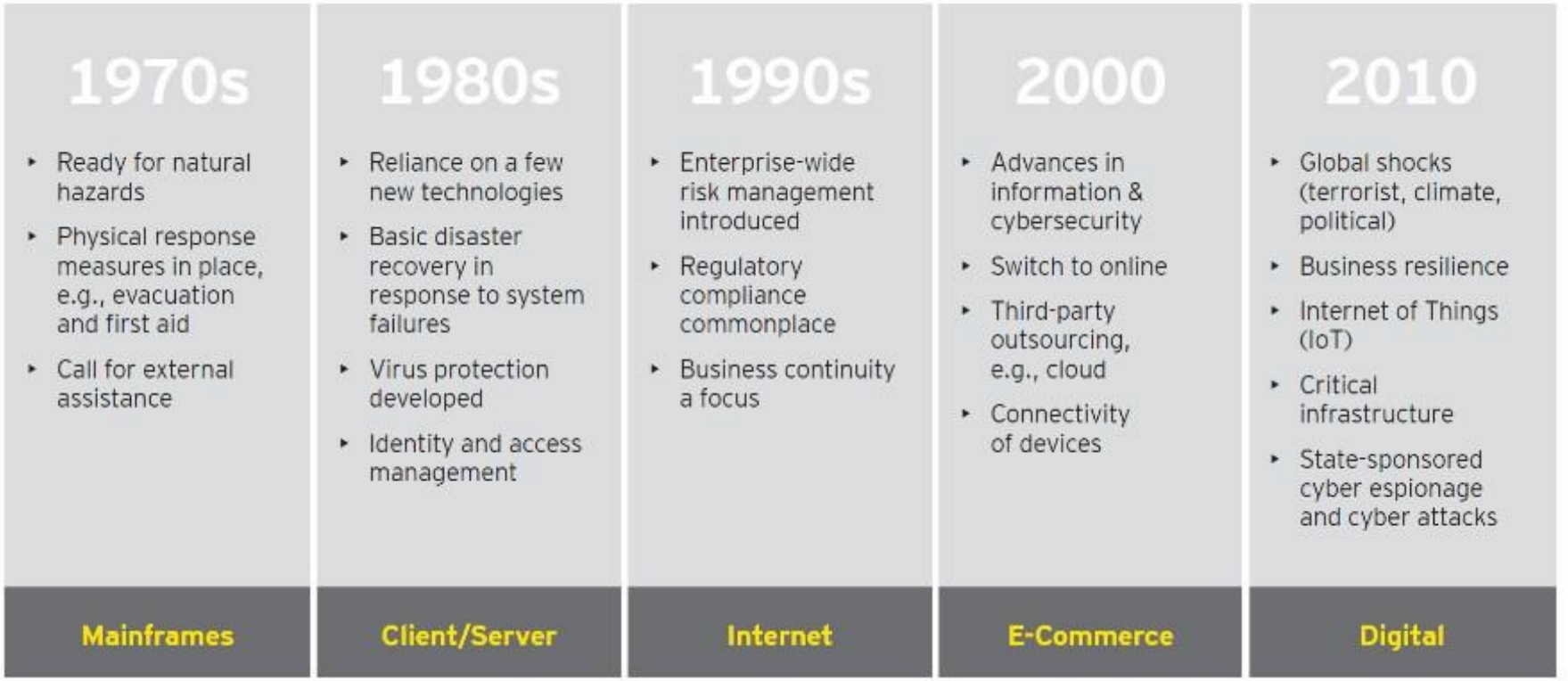
EY
Building a better working world

A secure organization is able to defend itself against cyber threats and withstand ongoing attacks.

A secure organization is **cyber resilient**.

Evolution

Organizations have learned over decades to defend themselves and respond better.



The components of cyber resilience

Sense

The ability of organizations to predict and detect cyber threats.

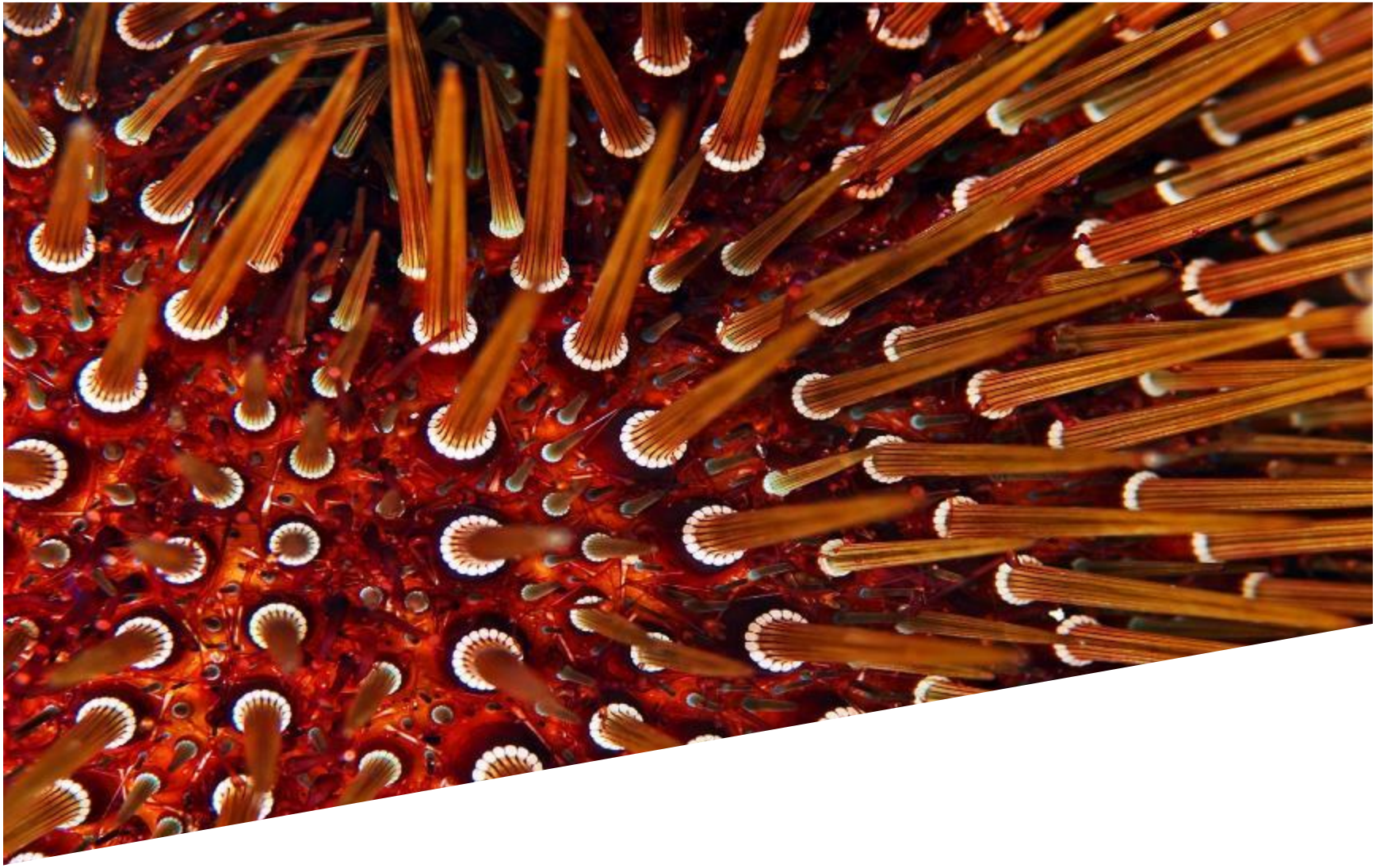
Resist

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

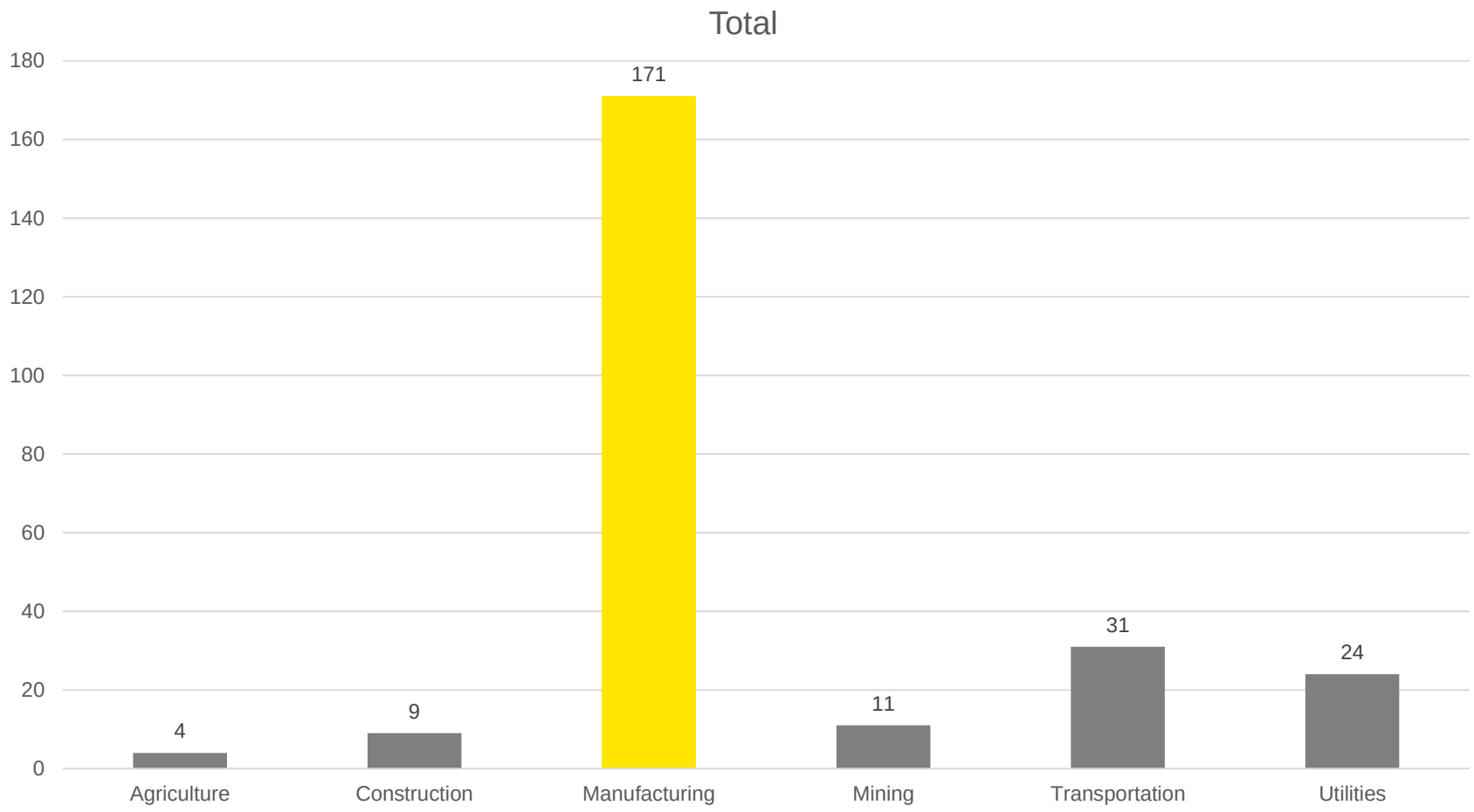
React

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

2016: Incidents. Findings. Trends.



Confirmed global cyber attacks against Industrial Sector organizations in 2016



Industrial Sector findings compared to the rest of the world

Industrial Sector

- **80%** in the Industrial Sector say that their cyber security function did not fully meet their organization's need
- **56%** of respondents in the Industrial Sector have had a recent significant cyber security incident
- **76%** in the Industrial Sector would not increase their cyber security spending after experiencing a breach which did not appear to do any harm.
- **75%** in the Industrial Sector do not have, or only have an informal, threat intelligence program.

World

- **86%** say that their cyber security function did not fully meet their organization's need
- **57%** of responders have had a recent significant cyber security indent
- **62%** would not increase their cyber security spending after experiencing a breach which did not appear to do any harm
- **64%** do not have, or only have an informal, threat intelligence program

Major findings for the Industrial Sector

- **92 %** of organizations in the Industrial Sector do not evaluate the financial impact of every significant breach.
- **46 %** in the Industrial Sector say that end user awareness, exploited via phishing is the primary control or process failure that lead to the most significant cyber breach in the last year
- **83 %** in the Industrial Sector see careless employees as the most likely source of an attack today
- **56 %** in the Industrial Sector do not have an agreed communications strategy or plan in place in the event of a significant attack

The biggest challenges in the Industrial Sector lies with security awareness and threat such as phishing

Priorities

- Business continuity, disaster recovery, resilience
- Insident response capabilities
- Security awareness and training

Threats

- Phishing
- Malware
- Cyber-attacks
- Zero-day attack

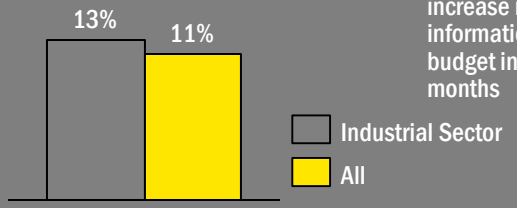
Vulnerabilities

- Careless or unaware employees
- Outdated information security controls or architecture
- Unauthorized access (e.g., due to location of data)

Triggers for increased budget

- Discovery of a breach that resulted in the attackers impacting the organization (73% likely-highly likely)
- DDoS attack (44% likely-highly likely)
- 46% of industry participants answered that budget constraints is a main obstacle in the adoption of IoT

Investments



% who expect > 25% increase in the total information security budget in the coming 12 months

Industry challenges

- More than half of the industry does not have an agreed-upon plan in place in the event of significant cyber-attack.
- Handling consumer data while expanding in to new areas of marketing i.e. social media, resulting in an increasing number of connected devices and a larger attack surface for cyber criminals

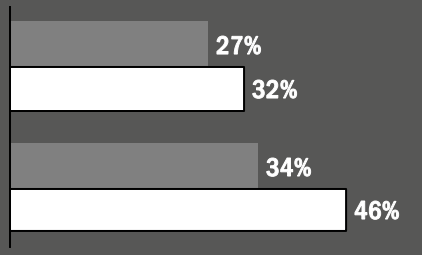
Least mature processes

- Metrics and reporting
- Third-party management
- Incident managemt

How is the Industrial Sector responding to identified industry trends

Phishing

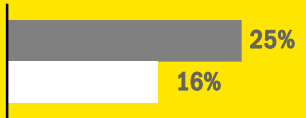
% of respondents that rank phishing as the threat that has increased their risk exposure the most over the last 12 months



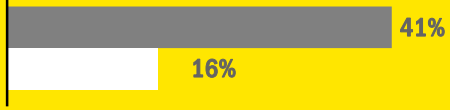
% of most significant cyber breach(es) that was due to end user awareness, exploited via phishing

Data protection - GDPR

% that will increase Privacy budget in the coming 12 months



% that have policies and procedures defined at group level or group level with corporate oversight



Security awareness

% that rank Security awareness and training as highest priority

% that will Increase Security awareness and training budget in coming 12 months

Internet of Things

% of respondents that have or are planning to implement a specific role or department for IoT connected Devices

% respondents that consider lack of skilled resources as the main obstacle in adopting IoT devices in the organization

Overall Industrial Sector

Recommendations for Improvement

Actions that will improve the Industrial Sector cyber security posture

Organizational structures

- Identification of actors responsible activities related to ICS-SCADA cyber protection
- Implementation of MS-own, more extensive structures divided into each critical sector

Assets covered

- Creation of definitions regarding when assets are considered critical
- Definition of critical infrastructure is based on the criticality of the services based on a risk analysis

Auditing and certification

- Auditing and certification right after developing definitions of critical assets and minimal security requirements
- Auditing and certification ICS devices and services providers

Incident handling

- Creation of inter-institution body responsible for ISC-SCADA cyber security incidents responses

Incentives

- ICS security assessments are performed on voluntary basis, sponsored by the Government
- Support commonly used by all CI operators.

Trainings and courses

- Cyber Security Advanced Courses in Control Systems and Industrial Automation
- Government collaboration with Academic institutions in the area of ICS SCADA cyber security

Contact

Carmen ADAMESCU
IT Advisory Partner
carmen.Adamescu@ro.ey.com

Vlad DONCIU
IT Advisory Manager
Vlad.Donciu@ro.ey.com

Sergiu SECHEL
IT Advisory Senior
sergiu.Sechel@ro.ey.com

EY | Advisory

About EY's Advisory Services

In a world of unprecedented change, 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.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities — strategy, customer, finance, IT, supply chain, people advisory, program management and risk — with a complete understanding of a client's most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory's high-performance teams also draw on the breadth of EY's Assurance, Tax and Transaction Advisory service professionals, as well as the organization's industry centers of excellence, to help clients realize sustainable results.

True to EY's 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital perspectives into every service offering.

EY Advisory's global connectivity, diversity and collaborative culture inspire its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to create innovative answers that help their businesses work better.

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

CONTACT

Carmen ADAMESCU
IT Advisory Partner
carmen.adamescu@ro.ey.com

Vlad DONCIU
IT Advisory Manager
vlad.donciu@ro.ey.com

Sergiu SECHEL
IT Advisory Senior
sergiu.sechel@ro.ey.com