Cyber trends in the market

Shelley Westman

Southeast Region Cybersecurity Leader, Ernst & Young LLP

Marcus C. Saiz de la Mora

Manager, Advisory Services – Cybersecurity, Ernst & Young LLP

Building a better working world

Presenters

Shelley Westman
Southeast Region Cybersecurity Leader
Ernst & Young LLP

Follow me @**ShelleyWestman**

Connect with me on **LinkedIn**

Marcus C. Saiz de la Mora
Manager, Advisory Services – Cybersecurity
Ernst & Young LLP

Connect with me on **LinkedIn**

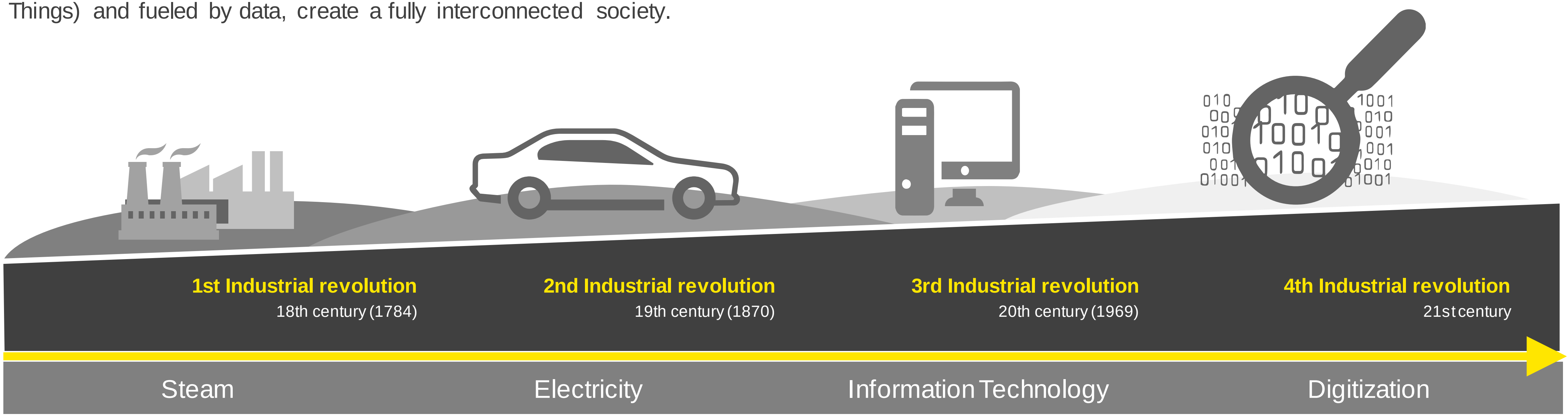
Agenda

- The transformative age
- Overview of disruptive enablers
- Robotics and artificial intelligence
- Internet of things
- Cloud security
- Data privacy and encryption
- Back to the basics

The Transformative Age is upon us

We are living in the Transformative Age. As depicted on the graphic below, we are in the 4th Industrial Revolution. We can expect a fundamental shift in everything we know, not only in the speed at which all these changes are taking place, but also in our increasing reliance on connectivity.

The **Transformative Age** can be described in two words: **Being Connected**. Today, cyber-physical systems, powered by IoT (Internet of Things) and fueled by data, create a fully interconnected society.



1st Industrial revolution
18th century (1784)

2nd Industrial revolution
19th century (1870)

3rd Industrial revolution
20th century (1969)

4th Industrial revolution
21st century

Steam

Electricity

Information Technology

Digitization

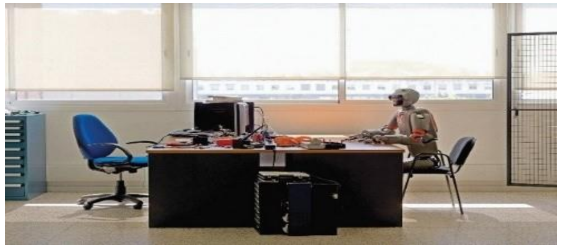
> “We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before”

World
Economic
Forum 2016

The impact of the fourth industrial revolution to companies today

2b

Jobs will be displaced by 2030
as a result of technology advances



20

Years to catch up with the cybersecurity skills shortage

29%

Unilever's CMO's estimated rate of click fraud, prompting a claim that the industry was wasting $8b–10b per year on fake clicks

4%

Of global group turnover — maximum fine for a data privacy breach in the European Union

Mega-vendors

Disrupters

Transformers

75%

Of the current run rate 75% of companies in the S&P 500 will be new entrants by 2027

** Source: "Digital Training/Playbook," EY website, https://go.ey.com/2BlbDM6, slide 35, accessed 2 October 2018.*

The importance and role of disruptive technologies in the Transformative Age

Influence rapid change

- Disruptive enablers are influencers on the Transformative Age
- Leveraging predictive data analytics and meta data to identify innovative solutions and drive predictability leads to timely problem solving

New business models

- New technologies and platforms (i.e., social media and mobility) are making companies change the way they operate and interact with their customers
- Disruption of the norm, which causes skills and traditional thinking to become obsolete

Impacting the bottom line

- Disruptive enablers have become essential for growth and allow organizations to create more value with less input
- Companies are seeing cost savings and efficiencies from RPA robotic process automation (RPA) enabling automation

Vulnerabilities and threats

- Device and endpoint proliferation has exponentially increased the attack surface for cyber threats
- Integration and growth of IoT are vastly increasing and complicating the networked landscape

As disruptive technologies go mainstream and are deployed, cyber complications must be addressed.

Cybersecurity controls and considerations in the Transformative Age

The rapid digitization across industries and sectors is leading to a dramatic increase in the number of cybersecurity incidents and data breaches. The facts and figures below put this into perspective …

$3.86m Average total cost of a data breach in 2018*

28% Likelihood of a recurring material breach over the next two years*

The disruptive technologies (listed below on the left side) present opportunities for operational efficiencies, frictionless user experience and consistency through automation. **With opportunities come threats**, and as such, it is imperative that companies **anticipate threats** by implementing **enhanced cyber capabilities**.

Robotics and artificial intelligence

- Automate and streamline business processes for strategic and operational efficiency while reducing cost

Internet of Things

- Enables physical devices to communicate and directly integrate across one common network

Cloud computing

- Allows companies to outsource computing resources rather than having to build and maintain computing infrastructures in house

Data privacy and encryption

- Protecting companies' sensitive data to comply with regulations and prevent financial harm

Cyber resilience activation

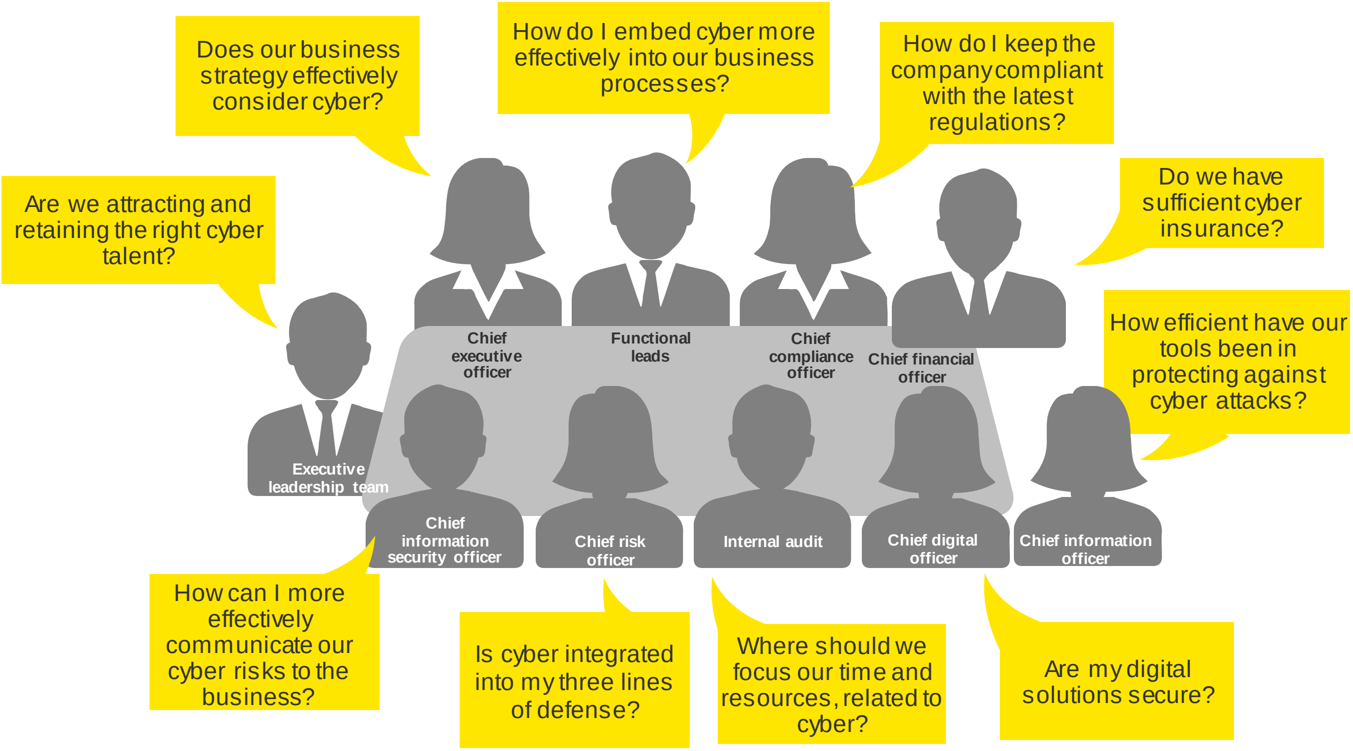
- Organizational capability to sense, resist and react to disruptive cyber events and recover in a timely fashion

Cloud security

- Maintaining the security of data in the cloud from theft, leakage and unauthorized access

* Source: "Cost of a Data Breach," IBM, 2018.

Cybersecurity is a topic at the forefront of board of directors concerns



Are we attracting and retaining the right cyber talent?

Does our business strategy effectively consider cyber?

How do I embed cyber more effectively into our business processes?

How do I keep the company compliant with the latest regulations?

Do we have sufficient cyber insurance?

How efficient have our tools been in protecting against cyber attacks?

How can I more effectively communicate our cyber risks to the business?

Is cyber integrated into my three lines of defense?

Where should we focus our time and resources, related to cyber?

Are my digital solutions secure?

Boards should focus on adopting the following as they relate to cyber risk:

- *Define and approve their cyber risk appetite*
- *Measure and evaluate cyber risk*
- *Develop more robust and transparent reporting*
- *Assign oversight across the board and via committees*
- *Overhaul cyber training for directors*

Robotics and artificial intelligence

Today, robotics is a critical component of an enterprise's digital strategy

What do we mean when we say **robotics**?

RPA **Robotic process automation**

- ► Robots that can be quickly trained and deployed to automate manual tasks across various business processes and to interact directly with a user interface with no need to develop code to automate individual tasks.

OR **Orchestration**

- ► Coding automation actions and actor modules with the goal of streamlining complex workflows and automating time-intensive tasks, follows a set of predefined rules that describe tasks and makes decisions based on criteria

CL **Cognitive learning**

- ► Incorporates machine learning and AI to process structured and unstructured data, aims to think and act the same way as humans do in order to perform complex tasks without human interaction

How can you **secure your robotics** ecosystem?

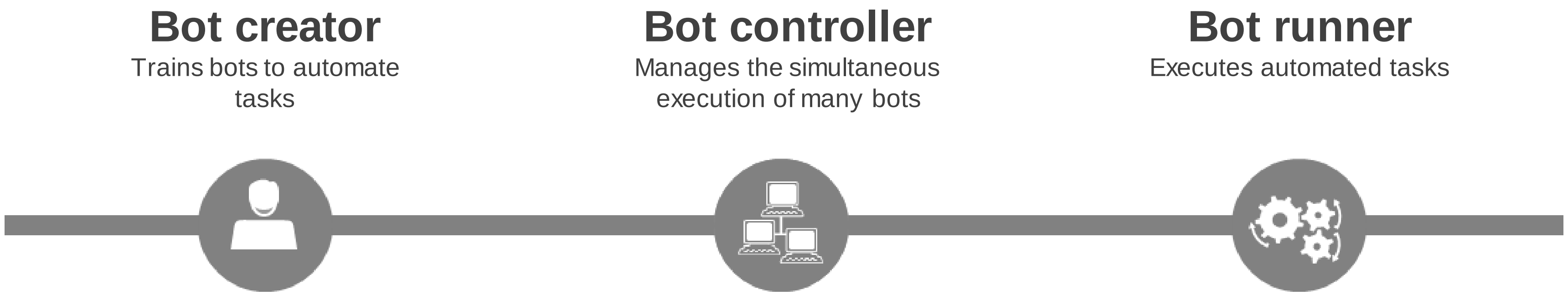
- ► Integrity: Can I trust that the data and results I get from my bots has not been modified or altered?
- ► Traceability: Am I able to monitor and track bot activities to identify the misuse of robotics affecting confidentiality, integrity or availability of other data?
- ► Confidentiality: Can I protect sensitive data from being purposely or accidentally disclosed by bot creators and bot runners?
- ► Control: Am I controlling access and protecting privileged accounts leveraged by the robotics system and users?

When it comes to securing a robotics ecosystem, an organization must consider the **technical**, **process** and **human elements** of the entire ecosystem.

Robotics introduces new risks to the environment

RPA introduces a new attack surface that can be leveraged to disclose, steal, destroy or modify sensitive data and/or high-value information; access unauthorized applications and systems; and exploit vulnerabilities to gain further access to an organization.

Detailed examples of robotics-related cyber risks that organizations should consider as they work to secure their robotics implementations include:



Bot creator
Trains bots to automate tasks

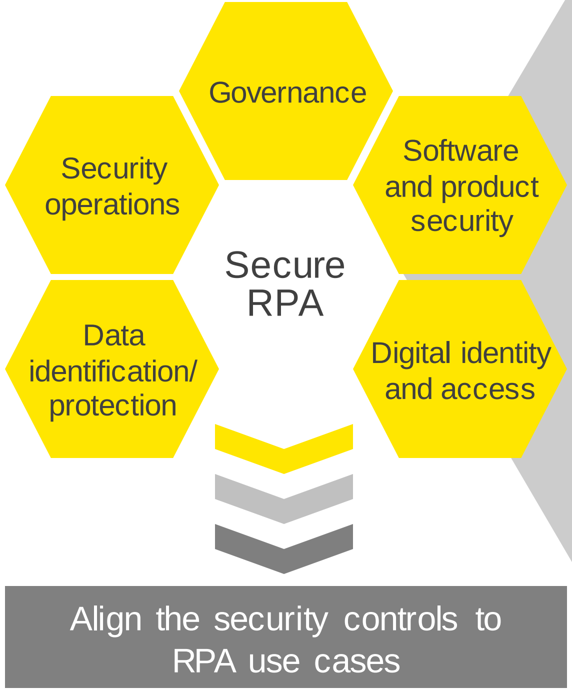
Bot controller
Manages the simultaneous execution of many bots

Bot runner
Executes automated tasks

Cyber risk	Scenario description
Abuse of privileged access	Attacker compromises privileged robotic user account to gain access to sensitive data and move through the network. A malicious insider trains a bot to destroy high-value data, interrupting key business processes.
Disclosure of sensitive data	A bot creator mistakenly trains a bot to upload credit card information to a database accessible via the web. A bot creator leverages a generic account to steal sensitive IP, leaving it difficult, if not impossible, to identify the true source of the leak.
Security vulnerabilities	A vulnerability exists in robotics software that provides attackers remote access to an organization’s network. A bot creator trains a bot to handle sensitive customer data but does not encrypt the transmission of that data to/from the cloud.
Denial of service	A bot is scheduled to execute in rapid sequence, resulting in exhausting all available system resources and halting all bot activities. A bot controller is disrupted because of an unplanned network, service, or system outage, resulting in lost productivity that is not easily replaced with human labor.

Establish controls to secure the RPA ecosystem

A secure design of an RPA ecosystem should include the entire product life cycle: requirements, selection, architecture, implementation and ongoing operations. Below are key security controls for considerations



Governance
Security operations
Software and product security
Secure RPA
Data identification/ protection
Digital identity and access
Align the security controls to RPA use cases

Governance	▸ Establish a governance framework with roles and responsibilities for securing robotics ▸ Build strategy and security requirements for RPA
Software and product security	▸ Perform security architecture risk analysis of chosen RPA solutions, including bot creation, control and running ▸ Integrate security scanning tools as part of bot creation
Digital and identity access	▸ Implement security controls to protect credentials during robotic session run time ▸ Manage user access privileges/segregation of duties risk
Data identification and protection	▸ Conduct compliance assessment to data regulations for use of robotics and automation ▸ Check the integrity of robotics and automation code
Security operations	▸ Gather log data from controller and bot runners to provide an audit trail of activities, monitoring for abnormal spikes in activity, access of systems and use of privileged accounts

Leveraging RPA and orchestration for security functions and tasks

Many CIOs and CISOs are challenged by hundreds of legacy technologies and applications that do not work well with one another. This leaves their teams to manually gather data from multiple systems, copy information from one system to another and switch between far too many applications to complete a single task.

The security functions within organizations are using these forms of robotics to:

- **Reduce time to detect and respond** to incidents, helping **minimize risk exposure** to an attack
- Close the talent gap by **automating resource-intensive tasks**, helping organizations manage operating expenses
- **Minimize employee turnover** due to lack of challenge or career progression by allowing employees to focus on higher-value tasks
- **Automatically deploy security controls** when vulnerabilities or compliance exceptions are discovered, resulting in a reduced attack surface
- Make **intelligent decisions quickly**, resulting in high-quality and consistent outcomes

We think robotics will help fill the anticipated talent shortage of 1.5m cybersecurity professionals by 2019.

Source: "(ISC)² Cybersecurity Workforce Shortage Continues to Grow Worldwide, to 1.8 Million in Five Years," (ISC)², February 13, 2017.

We believe robotics can help significantly reduce the average time to detect from the current 205 days, to weeks or even days.

Source: "The time it takes to detect an intrusion is critical for companies," Apcon, September 20, 2017.

90% of organizations feel vulnerable to insider threats.[1] We believe robotics can help by reducing employee exposure to sensitive data.

[1] "2018 Insider Threat Report," CA Technologies.

Internet of Things

Internet of Things (IoT) defined

Things

Things are the "smart" devices, products or sensors

Definition of a thing:

Any device enabled with an internet protocol that can exchange and communicate data

Data origination

Connectivity

Connectivity provides communication for the things

Definition of connectivity: Any interconnection for communication with the internet

Data interconnect

Infrastructure

Infrastructure enables people and businesses to connect to processes and systems data and the cloud

Definition of infrastructure:

Digital infrastructure or endpoints where data is used, process or stored

Data endpoint

Benefit of IoT: communications from things that are seamlessly connected to an infrastructure of users

The key driver for adopting IoT is improving operational efficiencies

The benefit behind all of the different reasons for IoT adoption is the communication of things, seamlessly connected to an infrastructure of users.

Many enterprises say they are using or expect to use data generated from their IoT solutions for objectives such as:[1]

- Improved customer experiences
- Supply chain visibility
- Improved safety
- Employee management
- Increased revenue

The Internet of Things could have an annual economic impact of $3.9t to $11.1t by 2025.[2]

[1] *"70% Of Enterprises Invest In IoT To Improve Customer Experiences," Forbes, November 2017.*

[2] *"What's new with the Internet of Things?" McKinsey & Company, May 2017, https://www.enterprise-cio.com/news/2018/jan/04/roundup-of-internet-of-things-forecasts-and-market-estimates-2018/.*

IoT barriers for adoption and vulnerabilities

90%

of consumers lack full confidence in the security of IoT devices.

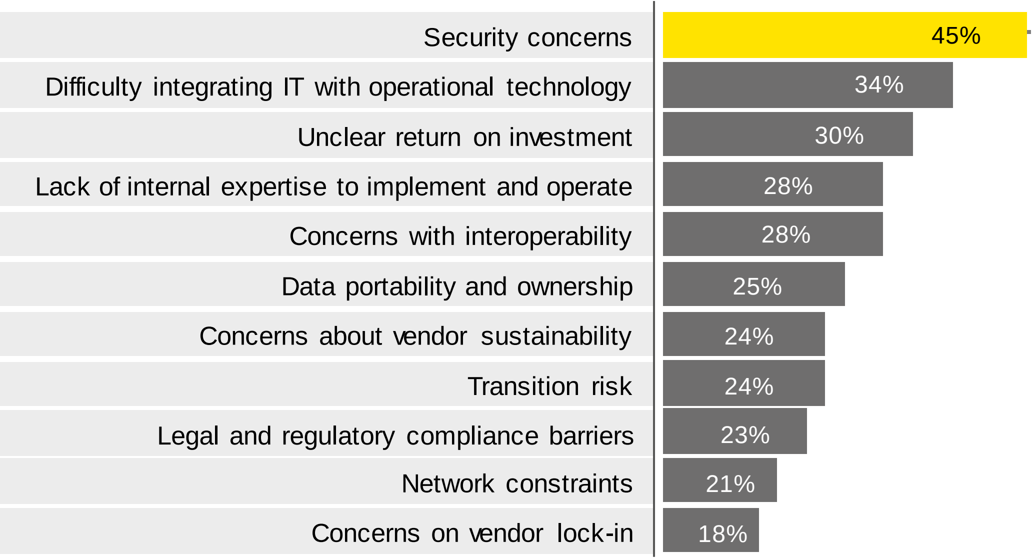
Source: "Gemalto survey confirms that Consumers lack confidence in IoT device security," Gemalto, October 2017.

Customers would pay **22%** more for security devices and would buy approximately **70%** more of them, which would boost the cybersecurity market by up to **$11b** in the year 2020

Source: "Cybersecurity Is the Key to Unlocking Demand in the Internet of Things," Bain & Company, June 2018.

Barriers to IoT growth, according to business executives

IoT barriers for adoption



Source: Bain 2018 IoT customer survey (n=521)

No. 1 barrier for adoption is security concerns

Cyber risks and IoT challenges

More connected …

25%

The IoT will be in the middle of at least 25% of identified cyber attacks by 2020.[1]

IoT security breach prediction

Forrester Research predicts that more IoT attacks will be motivated by financial gain than chaos. IoT-based attacks will likely continue to grow in 2018, including those on both devices and cloud backplanes, as hackers try to compromise systems for ransom or to steal sensitive information.[2]

Now a business risk

47%

of organizations rank the protection of data (company, customer, vendor, other) as the No. 1 critical driver for IIoT security.[3]

Growing IoT presence

Estimates indicate that IoT security spending will reach **$1.5b** in 2018 and is forecasted to reach **$3.1b** by 2021.[4]

Expanding vulnerabilities

The interconnectivity of people, devices and organizations in today's digital world opens up new vulnerabilities — access points where cyber criminals can gain access to sensitive data and systems. The scale of connected devices magnifies the consequences of insecurity.

[1] *"IoT Security: A Coming Crisis?" Trustlook, September 2017.*

[2] *"Forrester's top 6 cybersecurity predictions for 2018," Forrester Research, November 2017.*

[3] *"The 2018 SANS Industrial IoT Security Survey," SANS Institute, July 2018.*

[4] *"Worldwide IoT Security Spending Forecast (Millions of Dollars)," Gartner, Inc., March 2018.*

Once adopted, an IoT mindset can greatly affect organizations

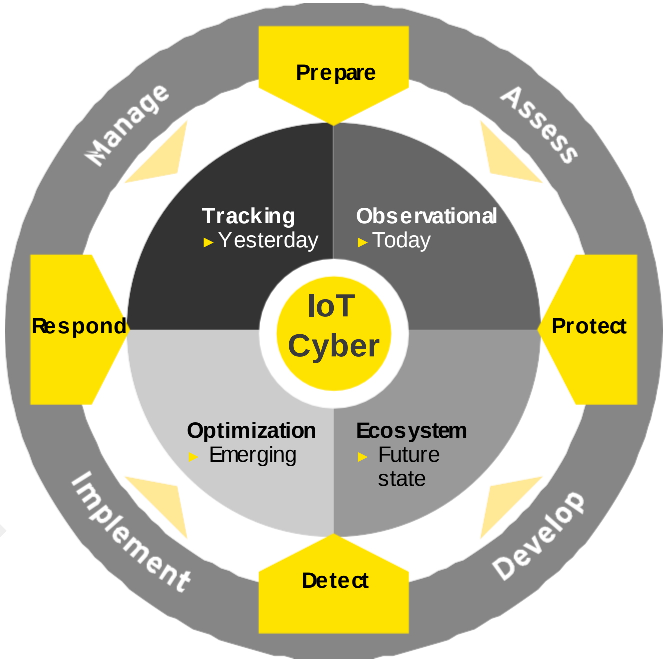
IoT is a game changer, impacting how you plan for the future of technology; the implementation and cybersecurity planning is not one-size-fits-all. All aspects of security must be examined.

Tracking

Today – tracking a single device; basic and fundamental approach; requires a road map that outlines a path to compliance and security integration[1,2]

Ecosystem

Future state – fleets of interconnected systems interconnected to suppliers, vendors and clients to optimize complete supply chain; fully utilizing the data collection, analytics and predictive analysis[1,2]



Observational

Tomorrow – tracking of devices plus web-based information and basic analysis; the evolution of the current systems, migrating to IoT[1,2]

Optimization

Emerging – fleets of devices that monitor and report to analytic platform(s) for process optimization; overlaying new IoT on existing system to leverage the gains of IoT[1,2]

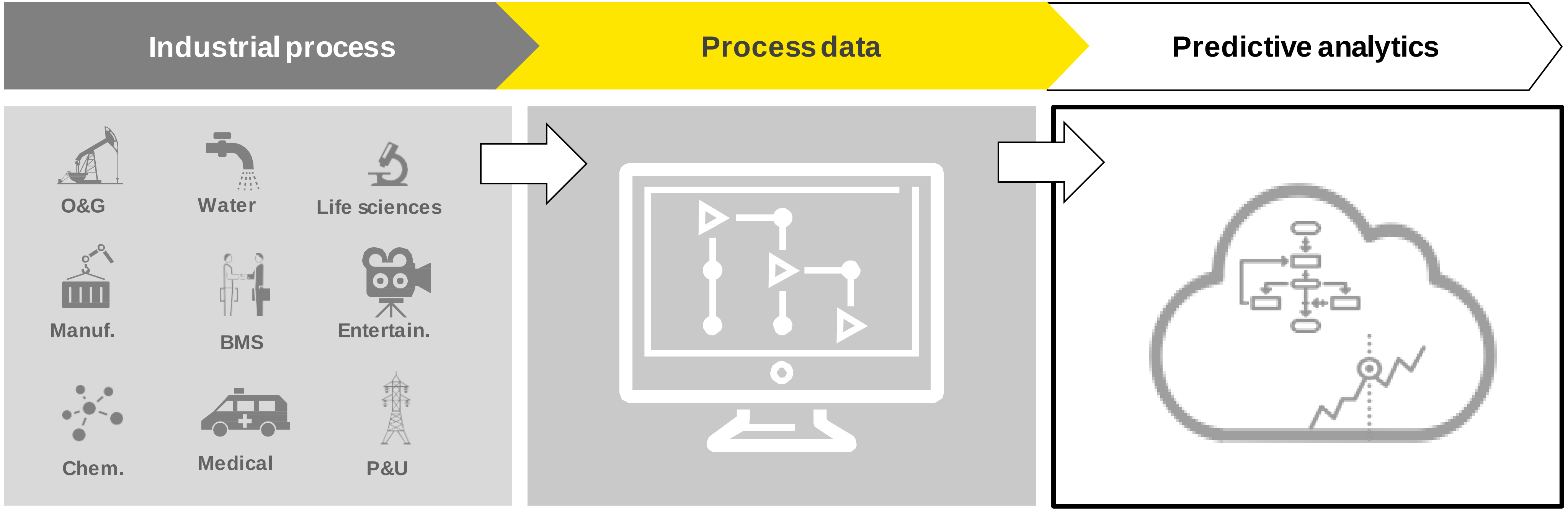
IoT cybersecurity strategies will be based on:

- Solid framework to identify risks
- Mapping risk to priorities
- Emphasizing data integrity
- Utilizing priorities to determine security controls

[1] 2018 Thales Data Threat Report.

[2] https://thenextweb.com/contributors/2018/04/27/12-big-encryption-trends-will-keep-data-secure/.

IoT data sent to the cloud for predictive analysis and insights



- Predictive analytics is the use of data, statistical algorithms and machine learning techniques to identify the likelihood of future outcomes based on historical data. The goal is to go beyond knowing what has happened to providing an assessment of what will happen in the future.
- To successfully realize these benefits, clients will need to:
  - Efficiently manage the volume, variety and velocity of IoT data
  - Employ sophisticated predictive analytics to accurately model IoT device performance
  - Adopt a predictive strategy to efficiently monitor, maintain and optimize their IoT offerings

Cloud adoption and security

Digital is increasing the pace of business transformation and cloud adoption

Business driver		Imperative and call to action
Environment	Multiple cloud service providers, greater attack surface	Need for **integrated, scalable** security capabilities to secure cloud services – not just a collection of controls – across multiple cloud service providers
Policy	Emerging compliance and regulations, additional complexity and cost	Since digital business models can change and expand overnight, you should require the use of **proven, repeatable** security design patterns to protect identities, data, IoT, “bring your own device,” etc.
Operations	Skills shortage, evolving security threats	Organizations are increasingly utilizing DevOps, requiring comparable agility from the security team, with **analytics and process automation** being key tenants of the security arsenal
Technology	Proliferation of security tools, limited integration and ROI	You need to shift from point security tools to implementing a **cloud security broker platform** to drive greater security visibility, effectiveness and ROI

Cloud services are becoming increasingly popular

Public cloud providers

Major cloud providers in the market include Microsoft Azure, Amazon Web Services (AWS), IBM Cloud, and Google Cloud Platform.[1]

61% of survey respondents are using more than one public cloud provider.

Plain text traffic

The benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.[2]

61% of organizations say they transfer sensitive or confidential data to the cloud whether or not it is encrypted or made readable via data masking or tokenization.

Enterprise cloud spending

Implementing additional cloud infrastructure security is costly. Public cloud spend is quickly becoming a significant new line item in IT budgets.

28% of key enterprise IT spending to be cloud based by 2022.[3]

Bring your own key (BYOK)

Bring your own key (BYOK) encryption is on the rise to protect cloud systems.

40% of companies have already implemented BYOK, and another 40% or so plan to implement it this year.

Cloud security

Enterprises voice mixed feelings about cloud infrastructure security, naming it both the primary benefit and challenge. This shows the importance of taking steps to ensure security, instead of relying on the cloud vendor.[4]

75% of enterprises implement additional security measures beyond what the cloud service providers offer, suggesting cloud security is not secure enough out of the box.

[1] "Global Encryption Trends Study," Thales, April 2018.

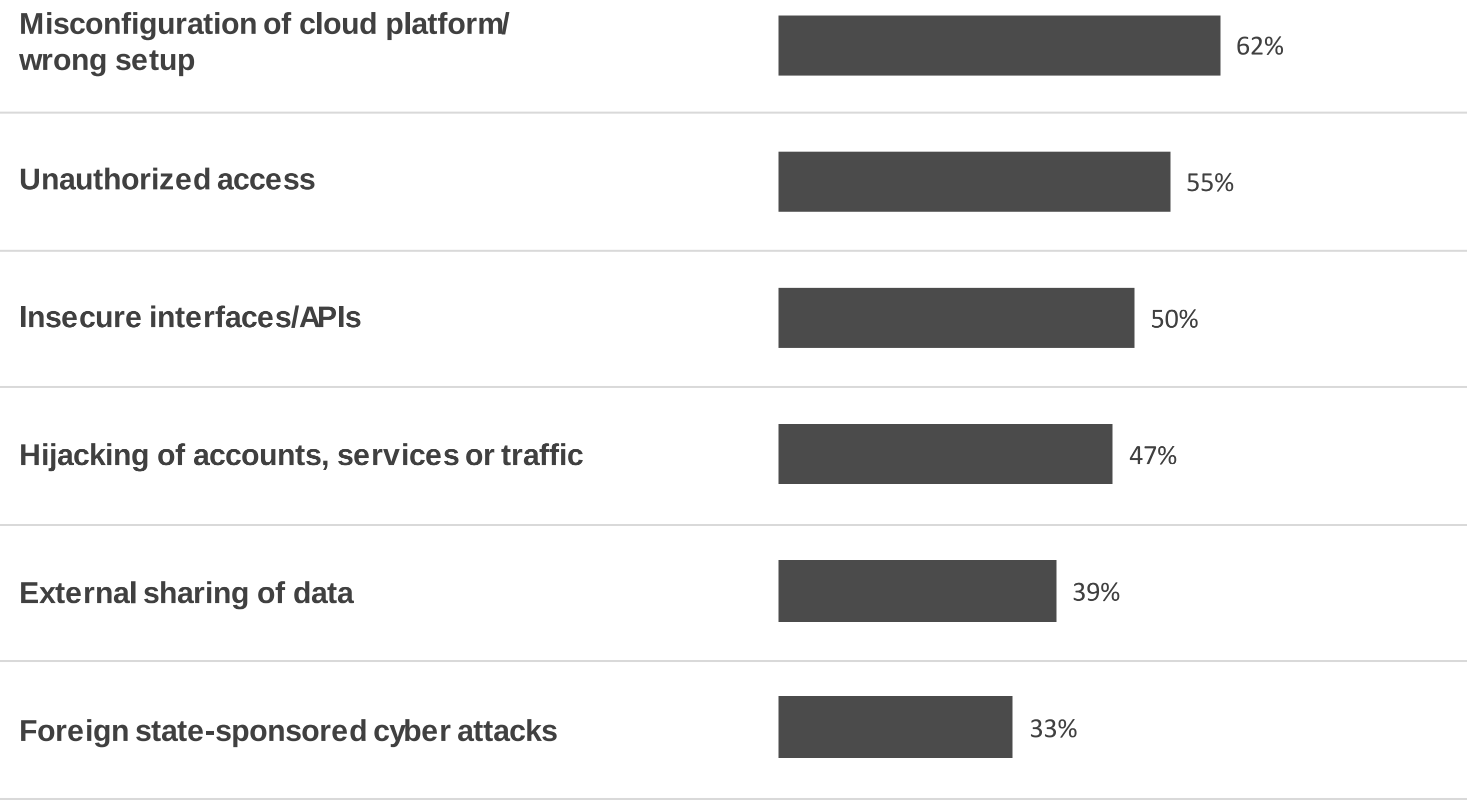
[2] ibid.

[3] "Almost a third of key enterprise IT spending to be cloud based by 2022, says Gartner," CloudTech, September 2018.

[4] ibid.

Cyber threats are evolving and cloud servers are a major target

What are the biggest cloud security threats for companies in public clouds?

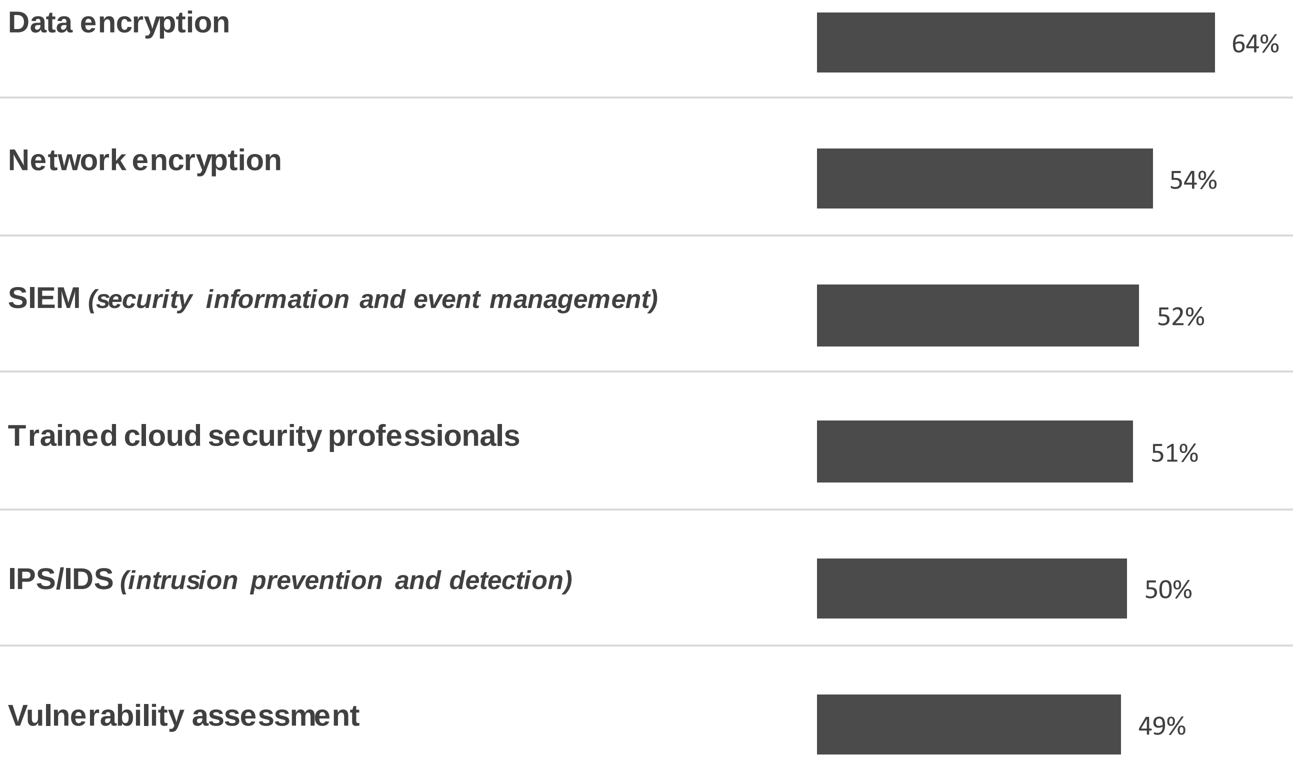


- Cloud misconfigurations have reached a point where sensitive data can't be protected with manual control.
- Insufficient identity, credential or key management can enable unauthorized access to data.
- These need to be designed to protect against accidental and malicious attempts to circumvent policy.
- With stolen credentials, attackers can often access critical areas of cloud computing services.
- Organizations lack awareness and visibility into external sharing in their cloud application and environments.
- Intelligence gathering, research and development, and intellectual property are targeted assets.

Source: 2018 Cloud Security Report, Cyber Insiders, 2018

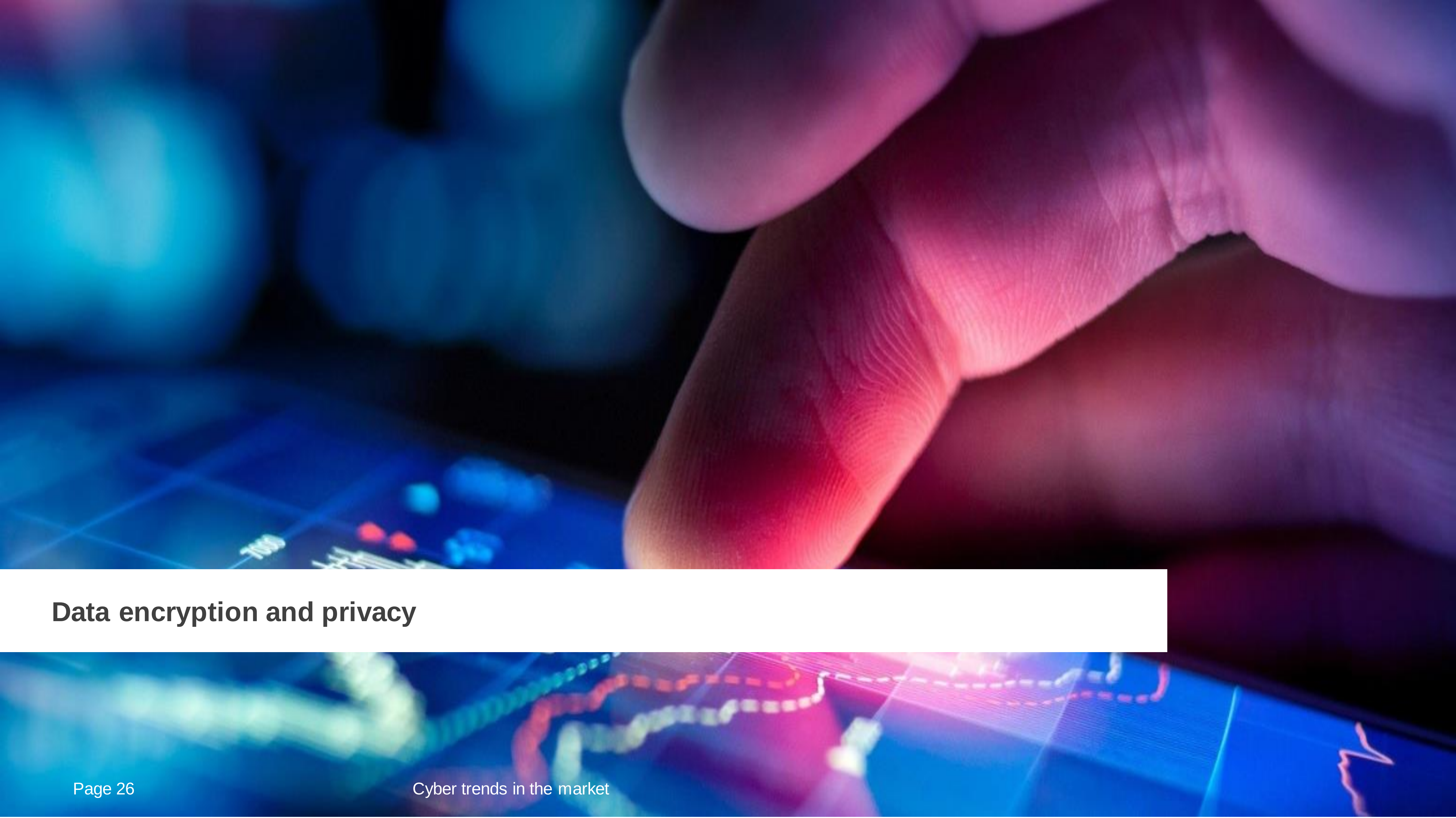
Leveraging cloud security technologies to address cyber risk

What security technologies and controls are most effective to protect data in the cloud?



- A barrier to a success data encryption program is the ability to understand where sensitive data resides
- The majority of organizations decrypt and then inspect SSL/TLS traffic looking for things such as malware
- Streamlined compliance reporting and incident handling through a centralized logging solution
- Clearly defined competencies and responsibilities drive accountability within the data security team
- Reduces the amount of network traffic reaching other security controls, resulting in reduced workload
- Identification of known security exposures before attackers find and exploit them

Source: 2018 Cloud Security Report, Cyber Insiders, 2018



Data encryption and privacy

Regulators seek to mandate accountability over data privacy

- Organizations are using social, mobile, big data and analytics and the IoT to gather as much information on customers as possible.
- Privacy protection used to be an afterthought, bolted on to information security programs in an ad hoc manner or not at all.

Financial impact: In addition to the potential penalties, companies face significant costs associated with internal churn created by uncertainty of compliance.

Business impact: Organizations have collected and stored massive amounts of data but have little understanding of what it is, where it's stored and what to do next.

What are some companies doing to address the new regulations?

- Align regulatory requirements and business opportunities.
- Assess business risks and readiness.
- Proactively manage the requirements to mitigate business risks and protect shareholder value.
- Implement appropriate data protection controls and technologies, such as encryption, to protect customer data.

Recent data privacy laws and regulations include the **EU General Data Protection Regulation** (GDPR) and the **California Consumer Privacy Act** (CCPA)

Understanding the market drivers for data encryption

Organizations are increasingly utilizing and deploying data encryption capabilities to meet privacy regulations and compliance requirements, keep pace with best practices and protect their most sensitive information.

Several major trends in today's market are shaping the use of data encryption, depicted below:

- Rise of insider threats is leading to a wider adoption of encryption in private clouds
- Compliance with regulatory requirements over the protection and privacy of data
- Understanding, discovering and classifying which sensitive data to encrypt remains a challenge
- Cloud computing needs outweigh risks associated with transferring sensitive data to the cloud

The use of encryption security services and technologies continues to steadily rise across all sectors in the form of symmetric and asymmetric encryption.

43%	of organizations now have a consistent enterprise-wide encryption strategy
12%	of respondents' IT security budget goes to encryption-related activities
57%	of respondents rate key management as very challenging
54%	of respondents use encryption to protect information against specific threats
44%	of respondents cite encryption as the top tool for increased cloud usage

Source: Global Encryption Trends Study, Thales, April 2018.

How organizations are currently viewing data privacy and encryption

Obstacles of encryption

- 67% of companies say that discovering where sensitive data resides within the organization is the biggest barrier to a successful encryption strategy[1]

Insider threats

- Privileged users were identified to be the top threat actor globally
- 77% of survey respondents worry about poor user awareness and behavior exposing them to risk via a mobile device[2]
  - The loss of such a device, and the potential for loss of information and an identity breach, are a concern for 50%

Willingness to change

- 68% of executives would not increase their information security spending even if a supplier was attacked — even though a supplier is a direct route for an attacker into the organization[3]

Most people may think that government-sponsored or organized cybercrime may be the biggest threat to sensitive data; however, employee mistakes are the most significant threat to sensitive data

[1] Global Encryption Trends Study, Thales, April 2018.
[2] *Cybersecurity regained: preparing to face cyber attacks — 20th Global Information Security Survey 2017–18*.
[3] "An integrated vision to manage cyber risk," EYGM Limited, 2017.

How many organizations plan on disrupting current encryption trends in the future

Predictions for big ideas in encryption technology[1]

- Cyber criminals are becoming more sophisticated, which quickly renders current technology irrelevant
- Developers are constantly striving to defensively disrupt current cybercrime trends with new technology

Homomorphic encryption

- Allows users to process data without decrypting it and produces encrypted results

Honey encryption

- Lets hackers think they guessed a password correctly by making it look like the information provided is accurate, but it isn't

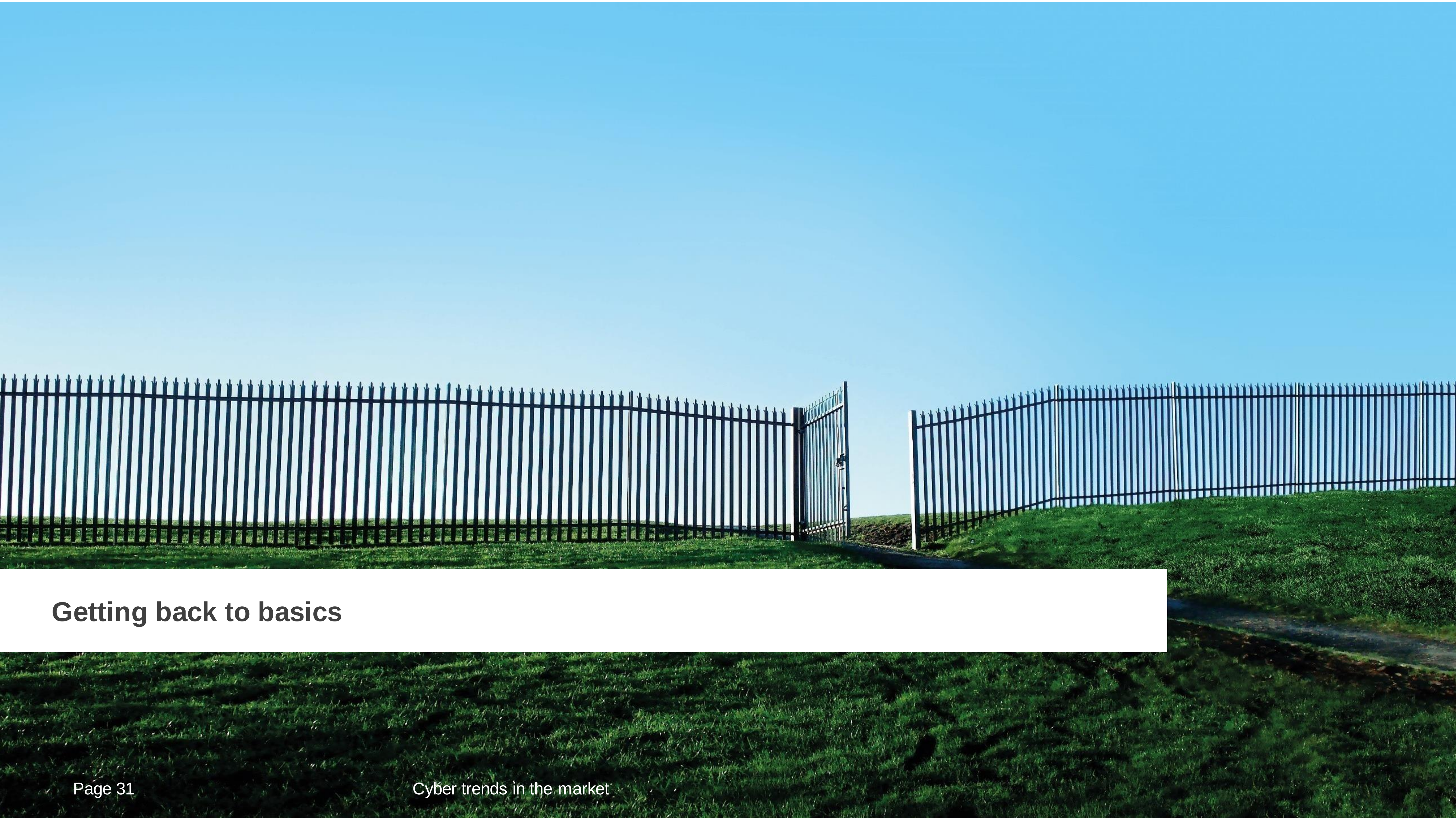
Quantum cryptography

- Uses photons of light to physically move a shared file between two parties
- The photons can't be cloned or copied

Moving target defense

- Constantly changes the attack surface so the bad guys can't spend time reverse engineering the environment

[1] *Scott Gerber, "12 big encryption trends that will keep data more secure," TNW, April 2018, https://thenextweb.com/contributors/2018/04/27/12-big-encryption-trends-will-keep-data-secure/.*



Getting back to basics

Understanding your organization’s threat landscape

If you do not understand the threats and the sort of harm they may cause your organization, then it will be very difficult to protect your environment from potential breaches and cyber attacks.

All organizations must assume that the worst could happen – there is no excuse for assuming otherwise. There have been too many well-known and worldwide attacks – such as Petya, WannaCry and Mirai – for complacency to be acceptable.

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.

The most likely sources of attack are still from within

- 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.
- The potential damage from losing a single smart device is understood to be increasing by 50% of respondents.

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

Source: EY Global Information Security Survey 2017-2018

If employees change their behavior and adopt basic cybersecurity hygiene, it should be possible to prevent an even greater proportion of common attacks.

Conclusion – getting back to the basics

Disruptive enablers sometimes come from years of work in corporate research and development labs, but most times, it’s the little things that leave organizations most vulnerable.

Organizations must understand and live by the fundamentals of cybersecurity. This means that the basics need to be implemented:

- Secure passwords
- Informed employees (phishing, USB drops, etc.)
- Proactive threat detection
- Controlled access (identity and access management)
- Business continuity and disaster recovery plans

Themes from cybersecurity investigations

It is rarely just about having the right technology

Most large breaches are the product of smaller, unmitigated incidents. For example:

- Attacker was detected early but the issue was never escalated, or the risk from the attacker was misunderstood. Therefore, the enterprise was left vulnerable.
- Attacker was detected early by security tools, but the response was insufficient.
- Security tools were purchased, but the company did not understand how to effectively leverage the tools or the tools were misconfigured.

Hygiene

The key to strong cybersecurity is excellent hygiene; new technologies grab headlines, but executing fundamentals is critical

IT general controls (ITGC)

Policy or process in place to provide reasonable assurance around the confidentiality, integrity and accuracy of system data.

Identity and access management (IAM)

- **Privileged access management**
  Strengthen protection and monitoring use of administrator credentials
- **Next-generation authentication**
  Enhancing requirements to connect to a network beyond usernames and passwords

Monitoring and response

Reviewing system activity for unauthorized access and anomalous behavior

Many (if not most) cyber breaches point back to failure of key "cyber fundamentals"

Digital asset management

Visibility into all securable assets

Identity and access management (IAM)

Differentially protect information assets that drive business goals and objectives

Monitoring and response

Fixing known vulnerabilities

> **"All compromise is based on give and take, but there can be no give and take on fundamentals. Any compromise on mere fundamentals is a surrender. For it is all give and no take."**
>
> **– Mohandas Gandhi**

Resiliency

Concerns about cybersecurity – and day-to-day operational resiliency – point to the need for a well-thought-out enterprise-wide resiliency strategy

1 Govern and challenge cyber resiliency

2 Risk-assess cyber resiliency

3 Identify, architect and protect systems

4 Manage critical third parties and other key dependencies

5 Detect, respond, recover and communicate

6 Test systems and recovery plans

What is resiliency?

The Department of Homeland Security defines resilience as **the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions**. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

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.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

US SCORE no. 04549-181US

1809-2899907. ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com