5 insights for executives

Can we trust them?

As digital technologies take hold, organizations need to understand and manage the risks to their valuable assets

Of special interest to
- Chief information officer
- Chief information security officer
- Chief risk officer

EY
Building a better working world

Digital technologies such as social, mobile, analytics and cloud are fundamentally changing how companies do business. Companies that use digital technologies successfully embrace them as part of their business and IT strategies, weighing the value as well as the potential risks. Yet, as digital's use expands across the enterprise, IT departments struggle to control and manage the proliferation of digital technologies within the organization, as well as the associated risks. They may improve the way we work, live and interact with one another, but can we trust it?

Building trust into an environment where digital technologies, legacy systems and infrastructure all have to live together in one digital ecosystem can be challenging. It requires organizations to rely more on third parties and expand the borders of the technology perimeter into places they cannot control. As organizations relinquish control, it is critical to assess the new risks they assume and find new ways to mitigate them.

1

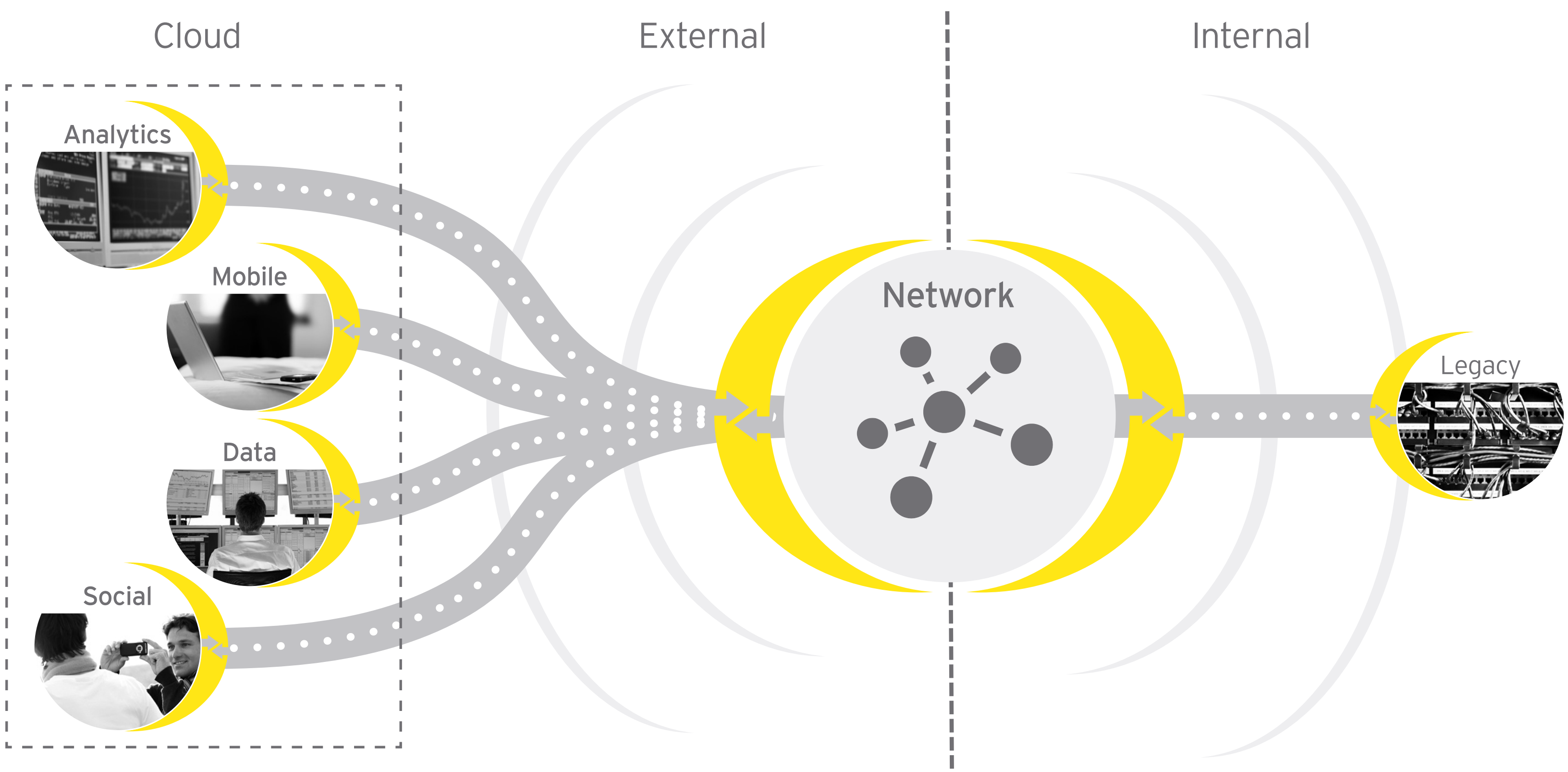
What's the issue?

As the perimeter of an organization continues to expand, its ability to manage technology diminishes. Digital technologies increase risk by allowing additional devices, new services and third parties access to the organization's systems and assets. This significantly extends the organization's IT footprint.

Traditional IT risk management and security acting as point solutions are not enough. Instead, organizations need to build a digital trust framework that expands their approach to perimeter-based cybersecurity. They need to break down silos, look across the complete digital landscape to assess new risks and make smarter risk-based decisions.

Digital technologies increase risk by expanding an organization's IT footprint.

Digital trust



2

Why now?

Businesses across all industries, as varied as agriculture, health care and automotive, are implementing digital technologies in creative ways to improve the way they work and serve their customers.

As more devices connect with one another in an ever-expanding realm known as the Internet of Things, digital technologies are acquiring the capability to gather, store, process and communicate information using sensors, embedded computing power and cloud services. Moving well beyond mobile phones and tablets, the Internet of Things includes watches, thermostats and kitchen appliances. Gartner projects the Internet of Things will consist of 25 billion devices in 2020, up from the 4.9 billion in 2015.[1] While many of these devices are consumer-focused, there are real business applications.

As digital technologies make it easier for us to access information, the number of ways cyber attackers can compromise an organization's security increases as well.

In short, the avenues of risk are growing faster than companies can react and remediate.

As digital technologies make it easier for us to access information, cyber attackers also gain more ways to compromise an organization's security.

3

How does it affect you?

A breach or loss of data, whether through a device or third-party service, can damage a company's brand, reputation and financial performance.

Without the appropriate governance in place, systems and sensitive information may be vulnerable. It is important for IT organizations to understand how the digital ecosystem is connected and how one vulnerability in specific area can lead to a compromise in many other areas. These technologies often do not require much technical expertise, so anyone in the organization can begin to use them without the assistance of IT. If sensitive information, such as intellectual property or customer personal data, is compromised, it may erode the confidence of consumers and investors and the organization's standing in the market.

As organizations become increasingly aware of their cyber risk posture, they will need to change the way they design and implement security programs to manage the risks that digital technologies represent.

A breach or loss of data can damage a company's brand, reputation and financial performance — perhaps catastrophically.

[1] Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities," Gartner, www.gartner.com/newsroom/id/2970017, 26 January 2015.

4

What's the fix?

Digital trust requires organizations to explore new ways of identifying and managing risks by combining new technology with established leading practices. Understanding what types of data they have and how it flows through their systems is not sufficient given the massive amounts of data organizations generate by the second. Instead, organizations need to consider how to use analytics more efficiently and effectively. They need to identify and manage the risks to their digital ecosystem so that they can better respond to threats as they arise.

Adopting digital technologies requires a holistic perspective — one that considers the implications of implementation across the entire ecosystem and builds security and trust into the digital strategy from the outset. As companies continue to connect more digital devices, they must include critical security and trust requirements during the development life cycle and then constantly validate their effectiveness.

Successfully identifying and managing risks/threats in your digital environment means you need to develop deep insights about your end users'—customers, employees, vendors, partners, etc.—experiences, behaviors, needs, and demographic attributes across multiple channels, services and devices. A feasible solution has to manage complexity while being cost efficient and scalable.

There are three steps organizations can take to build digital trust:

Identify

Organizations need to first understand how they are using digital technologies and how these technologies integrate with legacy systems before building a strategy to trust them. Digital technologies are already in use in most organizations, whether IT leaders want to admit it or not. Once organizations understand how digital technologies and services are being used, they can begin to identify risks and make risk-based decisions to implement controls and governance processes.

Integrate

Once organizations have identified the business needs for digital technologies and services, they should begin to integrate digital trust processes and controls into the digital ecosystem. Secure integration of digital technology requires organizations to understand the value of the information or systems involved, the third parties providing the technologies and services, the assurances they can offer, and any new implications presented by the technology (e.g., potential safety or privacy risks presented by connected vehicles).

Improve

Once operational, organizations need to monitor the use of digital technologies and services. Organizations must be prepared to quickly identify and respond to potential issues and make changes as needed. A well-organized digital ecosystem is constantly monitored and provides decision makers with updated information to reflect new risks in the environment. Customers expect companies to provide this level of support as risks evolve or change daily. If an organization fails to provide this support, customers will move to competitors or substitute technologies.

5

What's the bottom line?

Companies that successfully leverage digital technology embrace it as part of their business and IT strategies, weighing the value as well as the potential risks.

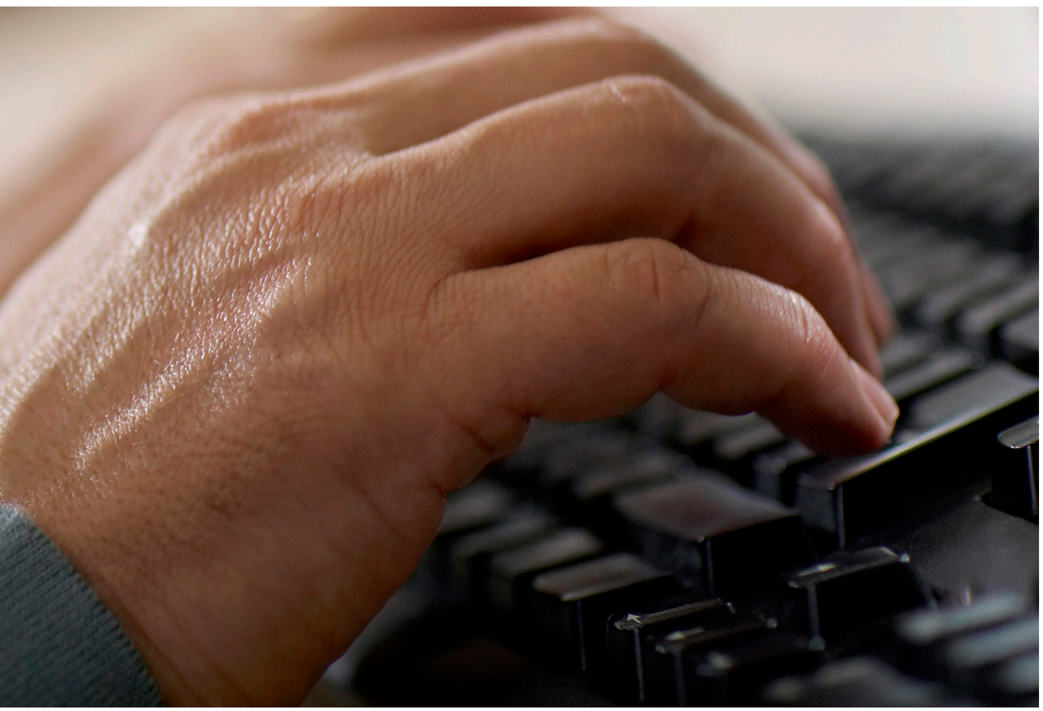
Conversely, companies that delay identifying, integrating and improving their digital ecosystems will miss new business opportunities and business efficiencies. They will often adopt digital technologies in an ad-hoc manner, creating the potential for security vulnerabilities that can open the door to breaches of sensitive data or systems.

The only way to fully rely on digital technologies is to have a trusted design, execution and certification. Organizations must continue to ask: How do we know we can trust our digital ecosystem? From there, they can take a proactive approach to build trust by mitigating risk in the digital ecosystem.

A digital trust framework allows companies to comfortably increase reliance on digital technologies and third parties.

Organizations must continue to ask: How do we know we can trust our digital ecosystem?

Want to learn more?



The answers in this issue are supplied by:

Justin Greis
Senior Manager
Ernst & Young LLP
+1 312 342 4202
justin.greis@ey.com

Fawaad Khan
Americas Cloud Leader
Ernst & Young LLP
+1 312 879 4314
fawaad.khan@ey.com

Greg Jenko
Principal
Americas Lead for Digital and Emerging Technologies
Ernst & Young LLP
+1 312 879 5392
greg.jenko@ey.com

Michael Schultz
Manager
Ernst & Young LLP
+1 214 969 8485
michael.schultz@ey.com

For related thought leadership, visit ey.com/5.

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.

About EY's Advisory Services
Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business having the right advisors on your side can make all the difference. Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

EYG/SCORE No. BT0472
ED None

ey.com/5

We want to hear from you!

Please let us know if there are subjects you would like *5: insights for executives* to cover.

You can contact us at:
fiveseries.team@ey.com