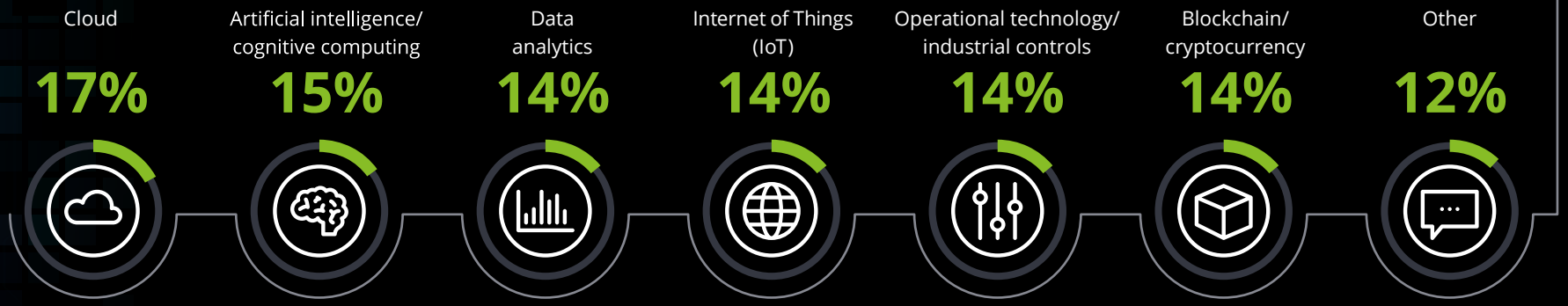
Deloitte.

# Tech Bytes Part 3: Cyber

Three things chief legal officers can do now to become more cyber-savvy

# Introduction




In the Deloitte & Touche LLP Future of Cyber Survey, responding C-suite executives indicated that they are prioritizing multiple digital transformation initiatives, not just one, to simplify environments and increase efficiencies.[1]

But that's not all. Organizations have been expanding their digital footprints, and thus their cyber exposure, for years within and outside their four walls, including, among others:

**Customers • Trading partners • Mobile workforces**

The reality today can be summed up in two words:

**Cyber everywhere**

# Yet there's a cyber disconnect developing

In the same 2019 Future of Cyber Survey, respondents noted that digital transformation is one of the most challenging aspects of cyber risk management.[2]

However, they said that their organizations are allocating

less than **10%**

of cyber budgets to these digital transformation efforts.

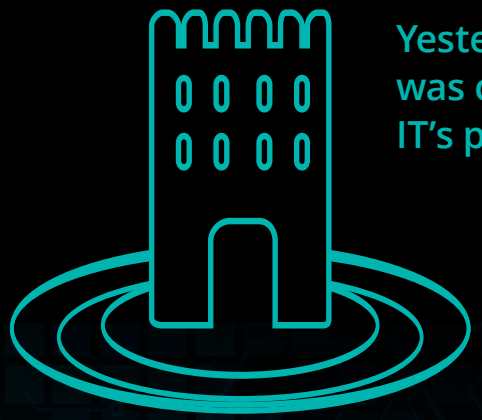
What's more, there appear to be notable gaps in organizational capabilities to meet today's cybersecurity demands. When asked about the most challenging aspect of cybersecurity management across organizations, respondents offered several perspectives:


For legal executives, these gaps should be of significant concern, because they could quickly escalate into incidents with potential operational, financial, regulatory, or reputational consequences.

⚠

Digital transformation = **Increased cyber risks**

# The cyber imperative for legal executives



## Yesterday, cyber was considered IT's problem

Just a few years ago, cyber was the domain of the IT department. At that time, cyber was generally viewed as securing the organization's networks and keeping intruders outside of a defensive perimeter. The legal department typically only became involved if there was a breach.

In a *cyber everywhere* world, cyber risks are everywhere, too. Each connected device is the new perimeter, each with its own potential for intrusion, disruption, and harm to the organization.

## With cyber everywhere today, cyber is everyone's problem

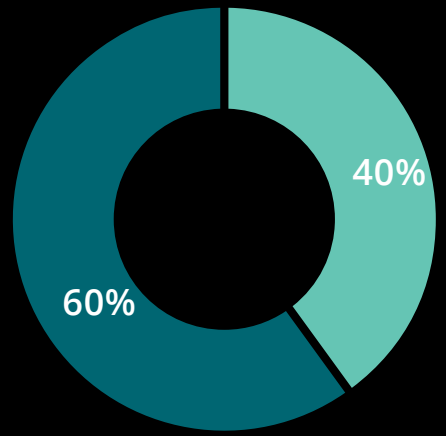
# The cyber imperative for legal executives

## Consider this

**Expanding regulations demand legal involvement**

- The European Union's General Data Protection Regulation
- China's Cyber Security Law
- India's proposed Personal Data Protection Bill 2019
- The California Consumer Privacy Act

Many legislative efforts around the world aim to protect data privacy and security. And that is just one facet of the rapidly changing global legal and regulatory environment involving cyber that has legal ramifications for organizations. How prepared is your legal department to understand and respond to these changes? A survey by Deloitte Touche Tohmatsu Limited and Oxford Economics indicates that 40 percent of legal departments don't have full visibility into legal and compliance obligations across all lines of business and functions.[3]



Legal executives can no longer take a reactive approach. In the following pages, we offer three interrelated actions legal departments can take now to be more:

**Knowledgeable • Proactive • Involved**

## Action #1

# Understand the cyber threat environment

Legal departments should be an active part of an organization's cybersecurity process from beginning to end. The first step is to understand the parameters of that process.

If you haven't already, **three key people** to engage with as soon as possible are:

- **CIO** (chief information officer)
- **CISO** (chief information security officer)
- **CRO** (chief risk officer)

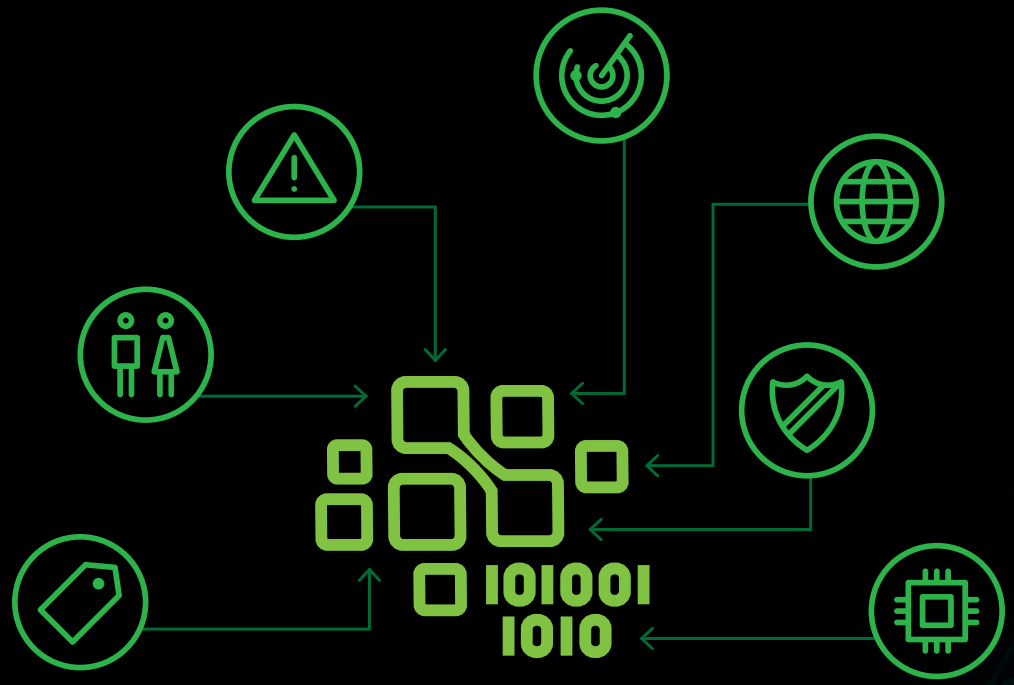
**Ask these questions** to help understand the scope of cyber threat environment:

- What are our digital crown jewels, the most important digital assets to our organization?
- Where do those assets reside, and who has access to them?
- What are potential digital paths to those assets (access points across the enterprise that pose the threat of intrusion, from within or from outside?)
- What data protection and privacy laws might affect how our organization shares data within or outside of our crown-jewel environment? Are we in compliance with them?
- Who are potential adversaries that might have interest in our digital crown jewels? What malicious acts might be perpetrated to gain access to them?

## Action #1

# Understand the cyber threat environment

## Consider this




The National Council of Information Sharing and Analysis Centers (ISACs) helps organizations in various industries share information that can protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. Members have access to information and tools to help them mitigate risks and enhance their cyber resilience.

## Action #2

# Look into the existing cybersecurity program

Most organizations today have some form of cybersecurity strategy. While knowing the technical details may be of some value, it can be more useful for legal executives to understand its scope and, at a high level, how effectively it addresses cyber risks the organization faces. In particular, you should be familiar with four areas of the cybersecurity strategy and the program in which that strategy is executed.

### Cyber risk profile

Understand the processes by which cyber risks have been identified and prioritized for your organization. How often is the profile updated? How does it account for a quickly evolving threat environment?

### Program governance

Assess who across the enterprise is involved in cybersecurity program oversight. Who sets policies and procedures? What internal controls are there for compliance? What resources and programs are in place to predict, detect, and respond to cyber incidents, and how much does the organization spend on cybersecurity annually? Are the programs insourced or outsourced? How are employees and business partners educated and trained about cybersecurity, and how is the effectiveness of that monitored over time?

### Cybersecurity safeguards

Determine what resources, both human and digital, are in place to defend the organization. How is the cyber perimeter defined? What security measures protect each type of device and the networks to which they have access?

### Cyber incident response and remediation

Identify existing disaster recovery plans for responding to data breaches and other cyber incidents and determine if they meet any applicable industry standards and regulations. If a breach occurs, what public disclosures and other actions are required? How quickly can the organization react to shut it down? Do existing plans go far enough not only in meeting requirements, but also to remediate the issue in such a way to build additional resilience so it's not likely to happen again?

## Action #2

# Look into the existing cybersecurity program

## Consider this

NIST Cybersecurity **Framework**

NIST Cybersecurity **Online Learning**

The National Institute of Standards and Technology (NIST) offers resources to assist organizations in understanding and improving their management of cybersecurity risk, including a Cybersecurity Framework resource for legal executives to learn more about cyber risk and determine the maturity of their organization's cybersecurity efforts vs. other organizations in the same industry.

## Action #3

# Apply a legal point of view

With a clearer view of the cyber threat environment and the organization's program for addressing it, legal executives can look upstream to determine where legal should be involved, both strategically and in discrete activities.

### Strategically

Bring a legal perspective to the cyber risk assessment, prioritization, and mitigation process. Have an active voice in how the organization views cyber risk and how key elements of a cybersecurity program address those risks. As the organization expands its cyber footprint into new geographic areas, stay on top of legal and regulatory implications.

### Tactically

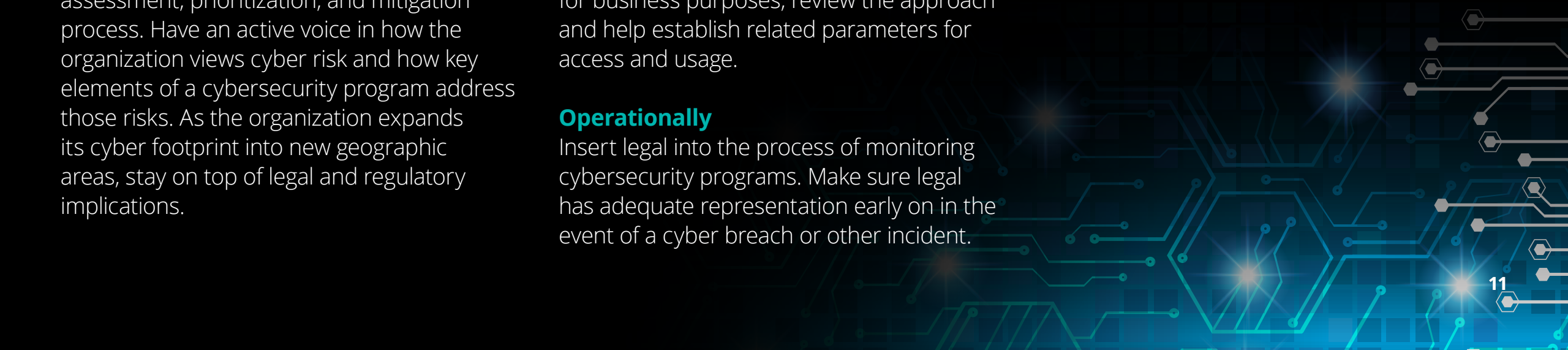
As new business initiatives are undertaken (for example, new product development, digital expansion into new markets, third-party relationships, and many others), take a seat at the planning table to represent the legal point of view. For example, if an organization allows employees to use company-owned or their own mobile devices for business purposes, review the approach and help establish related parameters for access and usage.

### Operationally

Insert legal into the process of monitoring cybersecurity programs. Make sure legal has adequate representation early on in the event of a cyber breach or other incident.

Play a more active role in remediation efforts to help mitigate risk to the organization and prevent similar future events.

To enable more effective strategic, tactical, and operational engagement, consider deeper training in cyber issues for your legal department or a subset of the department.



# If it's cyber everywhere, legal should be there, too

Legal executives and corporate legal departments are under growing pressure to elevate the strategic services they offer to the enterprise. With digital transformation as a top priority for many organizations and the scope of that transformation continually widening, doesn't it make sense for the legal department to be not just up to speed, but also an active participant in the transformation?

You can do that by becoming more knowledgeable about the cyber threat environment, being more proactive in wrapping your arms around the organization's approach to cybersecurity, and being an active contributor to that program by bringing the legal perspective to strategic, tactical, and operational decisions.

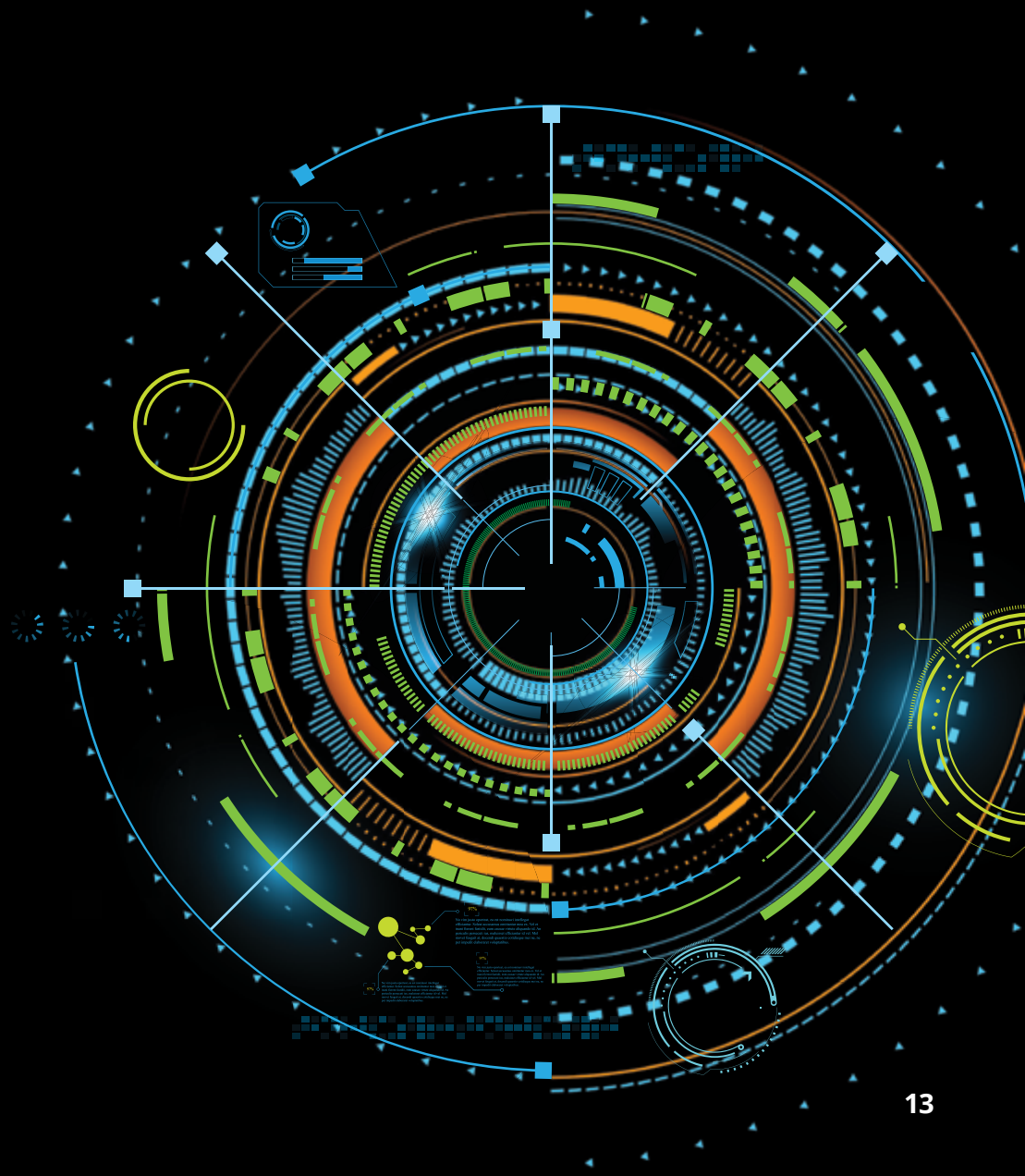
There's an added benefit to this more hands-on approach as well. As the legal department goes through its own digital transformation in the coming months and years, legal executives and the department will be both more knowledgeable about and better equipped to address their own cyber risks.

# Let's start the conversation

To learn more about cybersecurity and the legal department of the future, visit us at deloitte.com or contact:

**Lori Lorenzo**
Research & insights director
Chief Legal Officer Program
Deloitte Transactions and Business Analytics LLP
lorilorenzo@deloitte.com

**Acknowledgments**
Special thanks to Samir Hans, Chris Knackstedt, and Kiran Mantha for sharing their perspectives and insights.



# Endnotes

1 Deloitte Development LLC, 2019 Future of Cyber Survey, 2019
2 Ibid.
3 Oxford Economics and Deloitte Touche Tohmatsu Limited, unpublished research undertaken as part of Optimizing Value from the Legal Team, May 10, 2018

Deloitte.