Deloitte.

The CLO strategist: Cybersecurity

A framework for CLOs to lead in developing an effective cyber strategy

Introduction

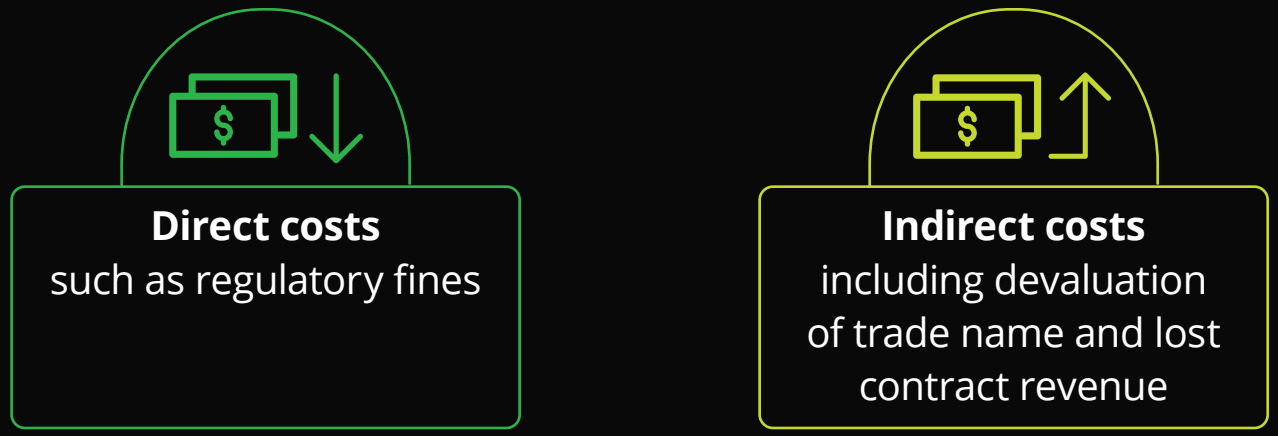
On a Sunday in December 2020, the federal Cybersecurity and Infrastructure Security Agency (CISA) issued an ominous warning. Hackers, the agency said, had exploited a network-monitoring platform from Tulsa, Oklahoma-based software company SolarWinds to breach computer systems in multiple government agencies. In the weeks that followed, it became clear that the attack affected a broad cross-section of public- and private-sector organizations and may have left sensitive data exposed for months. It was one of the worst episodes of cyberespionage in US history.[1]

Although the SolarWinds attack was remarkable in its scale, cyber incidents and breaches are common—and the threat is growing. Among C-level executives:

72% of survey respondents say their organizations experienced between one and 10 cyber incidents and breaches in the previous year alone[2]

69% report an increase or significant increase in threats to their business between early 2020 and May 2021[3]

Security breaches can lead to:



The direct costs typically associated with cyber incidents are less than those of indirect costs like brand impact. These costs play out over years, rather than months; in fact, more than 50% of associated costs accrue *after* year one.[4]

"CLOs can push their thinking about cyber strategy in terms of both innovation and execution, addressing the demands of today and looking to the journey ahead. Even CLOs who have been engaged to date by evolving the legal department to meet the organization's changing needs, supporting the growth of the business, and navigating regulatory and compliance requirements might ask themselves: What strategies should we develop to meet current and future challenges in this ever-evolving landscape?"

Deborah Golden, Principal,
US Cyber & Strategic Risk Leader,
Deloitte & Touche LLP

(Offense + Defense) Relationships = Strong Cyber Strategy

So what does a cybersecurity strategy mean from the CLO's purview?

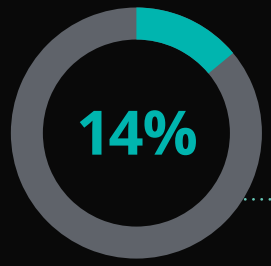
It means predicting, managing, and balancing risk. But it also means helping leaders across the organization develop offensive and defensive game plans so they can:

- Navigate the evolving regulatory landscape
- Manage cyberthreats more effectively, starting with areas of greatest risk and value to the business
- Plan for incident response so that it limits the impact of a data breach to the organization

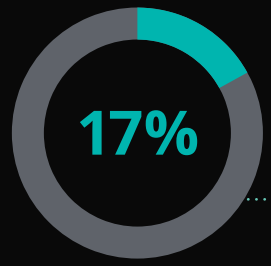
The CLO can develop a strong cyber strategy that is focused on both offense and defense, and empowered by cross-functional relationships. To do so, consider the five self-reinforcing choices.

For a deeper discussion of the five self-reinforcing choices, please see "The CLO strategist" overview article.[5]

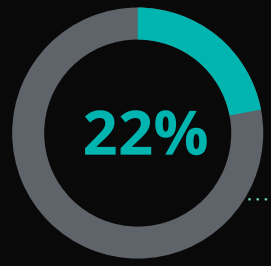
Biggest cyber incident impacts*



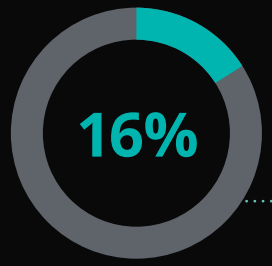
Loss of revenue



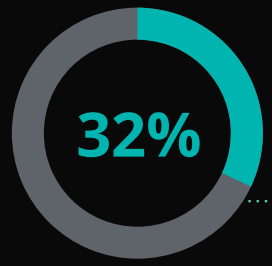
- Regulatory fines
- Reputational loss



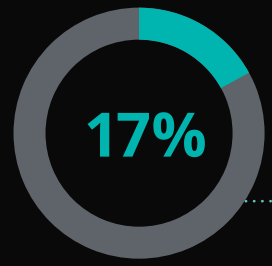
Intellectual property theft



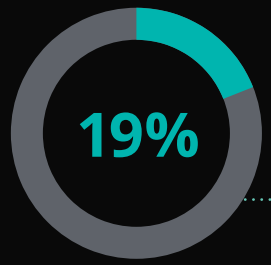
Negative talent/ retention impact



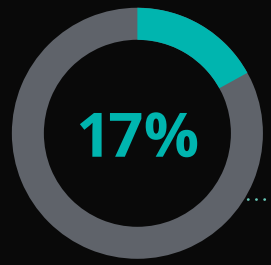
Operational disruption



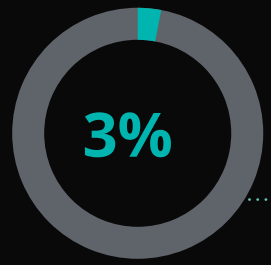
Change in leadership



Drop in share price



Loss of customer trust/negative brand



Other

*Respondents were asked to select up to two responses, so percentages will not add up to 100%

Source: Deloitte[6]

Developing an effective strategy involves tackling cybersecurity by process versus organizational silo. Consider, for instance, the track that a customer's data takes through the organization, from marketing and sales to finance to fulfillment and delivery—and that's a simplified view. A dynamic approach like this can help build consistency, transparency, and defensibility into legal governance, risk, and compliance.

Because it crosses functional responsibilities, a process-oriented approach to cybersecurity requires collegial relationships in areas such as:

Technology

Risk

Product management

Supply chain management

Compliance

Procurement

Business units

Marketing

Board of directors

"Collaboration is critical to a strong cyber position. The CLO is an ally to the board and other executives in the ongoing drive to secure assets and manage cyber risk. Collaborative relationships between and among Cyber and Legal executives is critical to effective cyber strategy."

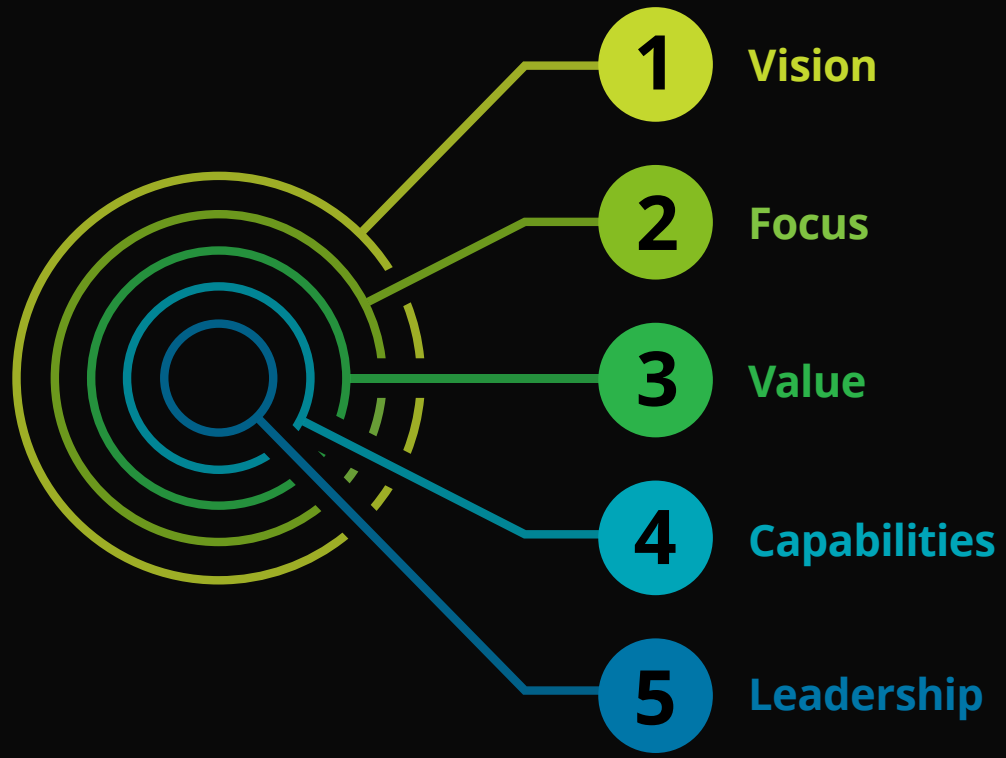
Deborah Golden, Principal,
US Cyber & Strategic Risk Leader,
Deloitte & Touche LLP

? Did you know?

According to the 2021 ACC Chief Legal Officers Survey, cybersecurity is the single most important business issue among CLOs.[7]

The five self-reinforcing choices

Strategy can be viewed as the result of five self-reinforcing choices, which we've adapted from Lafley and Martin's seminal guide:[8]



As a strategist, the CLO wears two hats:

Contributes to the enterprise strategy

Creates the strategy for the legal function

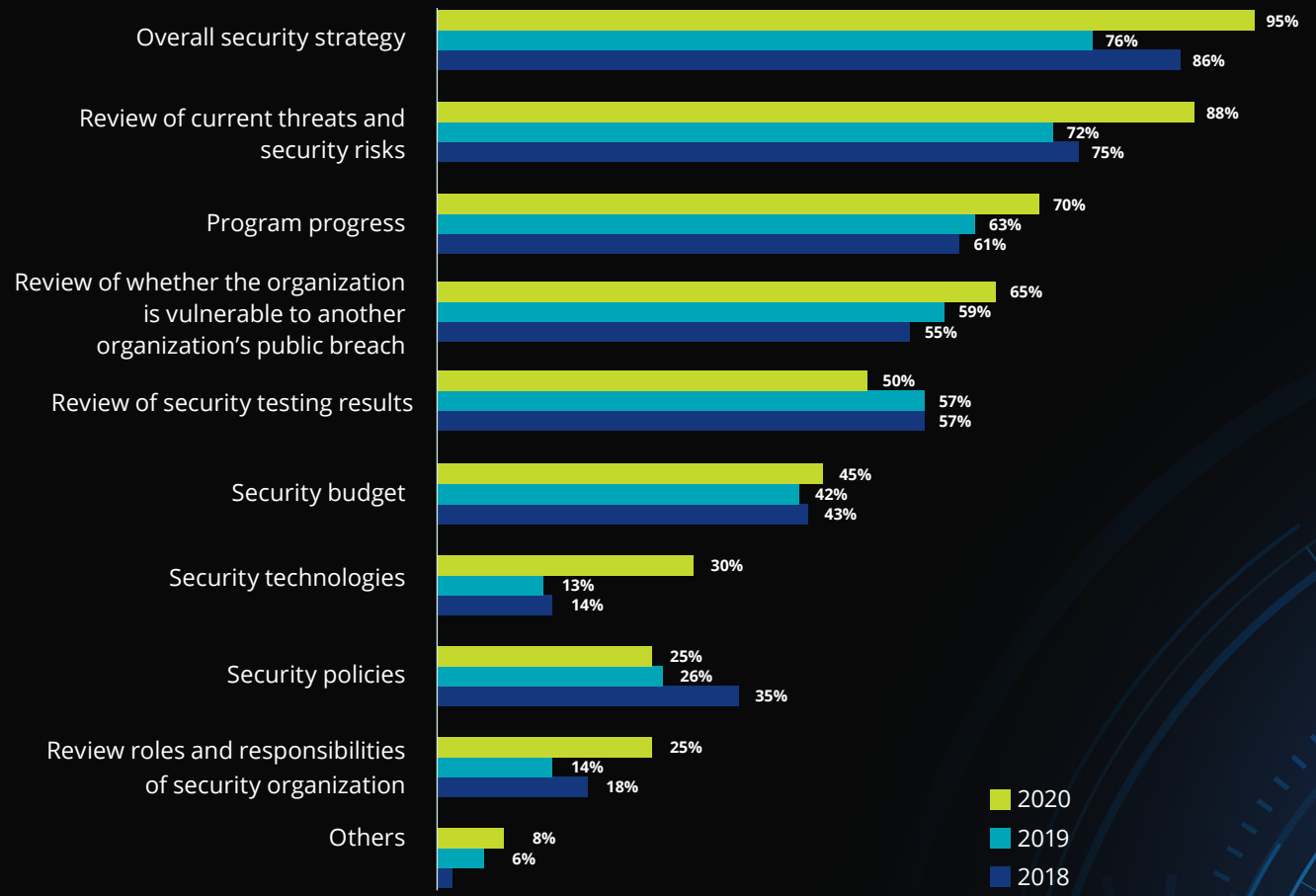
Let's look at cyber strategy through the lens of these five choices.

1 Vision

Articulate a sense of purpose, define your aspirations, and describe what success looks like.

As a **business advisor**, the CLO may seek to educate the board, senior management, and business unit leaders on the risks associated with a breach, the shifting regulatory environment, and the impact to the organization. At the same time, the CLO can learn from these same colleagues about the risks they're seeing.

Top cybersecurity areas of interest for board/management identified by survey respondents



Source: Deloitte[9]

1 Vision (cont.)

Articulate a sense of purpose, define your aspirations, and describe what success looks like.

This role involves helping leaders balance multiple dimensions of risk in the context of market and business realities, including:[10]

- The potential impact of regulatory proposals and changes across the various jurisdictions in which the company operates or seeks to operate
- The potential effects of a security event
- A response and mitigation strategy
- The cyber implications of third-party dependencies, data flows, and access
- Cyber governance, including roles and responsibilities

In addition, relationships and listening are critical. By fully integrating with leadership across the organization and endeavoring to understand specific business or functional considerations, the CLO can determine where the organization's opportunities and vulnerabilities may lie. The credibility built through a focus on relationships also positions the CLO to proactively work with business leaders.

Communicating the vision involves regular, plain-English updates on:

- Risk and strategy (to each stakeholder and to individuals within the organization at all levels)
- Regulatory and compliance changes (to leaders across the organization)

1 Vision (cont.)

Articulate a sense of purpose, define your aspirations, and describe what success looks like.

As the **legal function leader**, the CLO may seek to educate the function about cybersecurity and set a clear strategy for the function relative to that risk. For example, the legal team can make cyber "hygiene" a standard part of vendor contracts and work with the information security and marketing teams to develop standards for protecting customer data. Each member of the legal team should seek to understand how to recognize cyber risk within their area of expertise.

In either role—**business advisor** or **legal function leader**—when setting the vision, the CLO may want to:

- Engage multiple perspectives
- Frame the issues
- Lay out a plan

Did you know?

Across industries, board members consistently rank cyber as one of the top three risks confronting the enterprise.[11]

2 Focus

Clearly define what you will and won't do.

As a **business advisor,** the CLO may seek to untangle the rapidly evolving legal and regulatory framework around cybersecurity, reducing ambiguity for business colleagues internally as well as providing feedback to regulatory agencies externally.

A starting point is to help the organization understand its vulnerabilities:

Many organizations are unprepared to deal with cyberthreats that specifically target the most valuable digital assets with novel techniques that use the organization's strengths (such as strategic alliances) against them.[12]

The CLO can:

Help strengthen protections through the contracting process with alliance partners.

Even with a formidable security program, incidents can still occur. And when they do, they may go undiscovered for a long time while causing real, lasting damage.[13]

The CLO can:

Train the legal function to recognize cyber risk, proactively find ways to enhance protections across all functional legal areas, and team with other leaders on tabletop exercises to test the response to a breach.

Cyber programs often lack maturity across the threat life cycle, with greater focus on prevention versus response and resilience measures.[14]

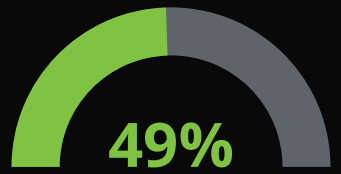
The CLO can:

Prepare the legal department to do its part through recurring training in cyber incident response, active participation in crisis planning, shoring up contract compliance, and systematically assessing cyber maturity relative to peers.

2 Focus (cont.)

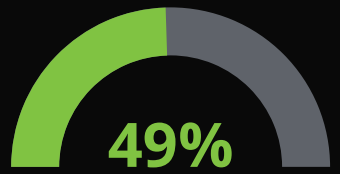
Clearly define what you will and won't do.

It's not unusual for business leaders—and even CLOs themselves—to be surprised by the magnitude of a cyber breach's impact. For example, only:



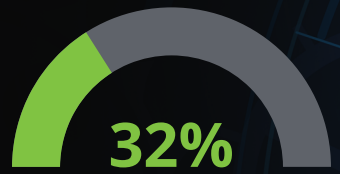
49%

of surveyed board members say their companies engage in monitoring or internal communications to detect trouble ahead[15]



49%

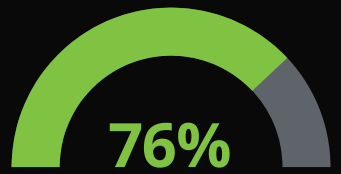
say their companies have playbooks for likely crisis scenarios[16]



32%

say their companies engage in crisis simulations or training[17]

But at the same time:

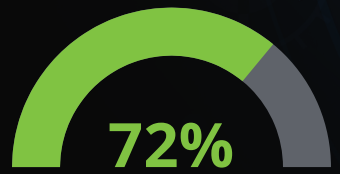


76%

of board members believe their companies would respond effectively if a crisis struck tomorrow[18]

85%

of chief marketing officers say they can measure and demonstrate compliance with global data privacy regulations[19]



72%

of legal executives are confident about the execution of their organization's plan to handle a cyberattack[20]

2 Focus (cont.)

Clearly define what you will and won't do.

As the **legal function leader,** the CLO may seek to enable the legal function to add value where the legal perspective can be most helpful. This includes issues of regulatory change and compliance. But it may also extend to insurance and managing risk in the third-party contracting process.

For example, insurers are starting to take a harder stance on cyber and decline to cover certain types of cyber risk. One carrier has recently revised its cyber insurance policies to exclude damages from "cyber war" between nation-states.[21]

As for contractual obligations, the legal function may want to reevaluate platform and connectivity service contracts across the organization to lay out what the expectations are with respect to cybersecurity—then do the same for the legal department's own relationships with law firms, service providers, and other outside parties.

2 Focus (cont.)

Clearly define what you will and won't do.

25%

of surveyed law firms say they have been hit with a security breach[22]

However, law firms can be slow to adopt security tools.

43%

use file encryption[23]

39%

use email encryption[24]

26%

use whole/full disk encryption[25]

3 Value

Identify the differentiated contributions that enable competitive advantage.

As both **business advisor** and **legal function leader,** the CLO and legal team can lend risk-sensitive legal and regulatory perspective in areas where risks are increasing or changing, taking care to consider not only how to respond to current risk, but also how to position the organization to proactively avoid or address risk in a forward-looking way. Consider some of these areas:

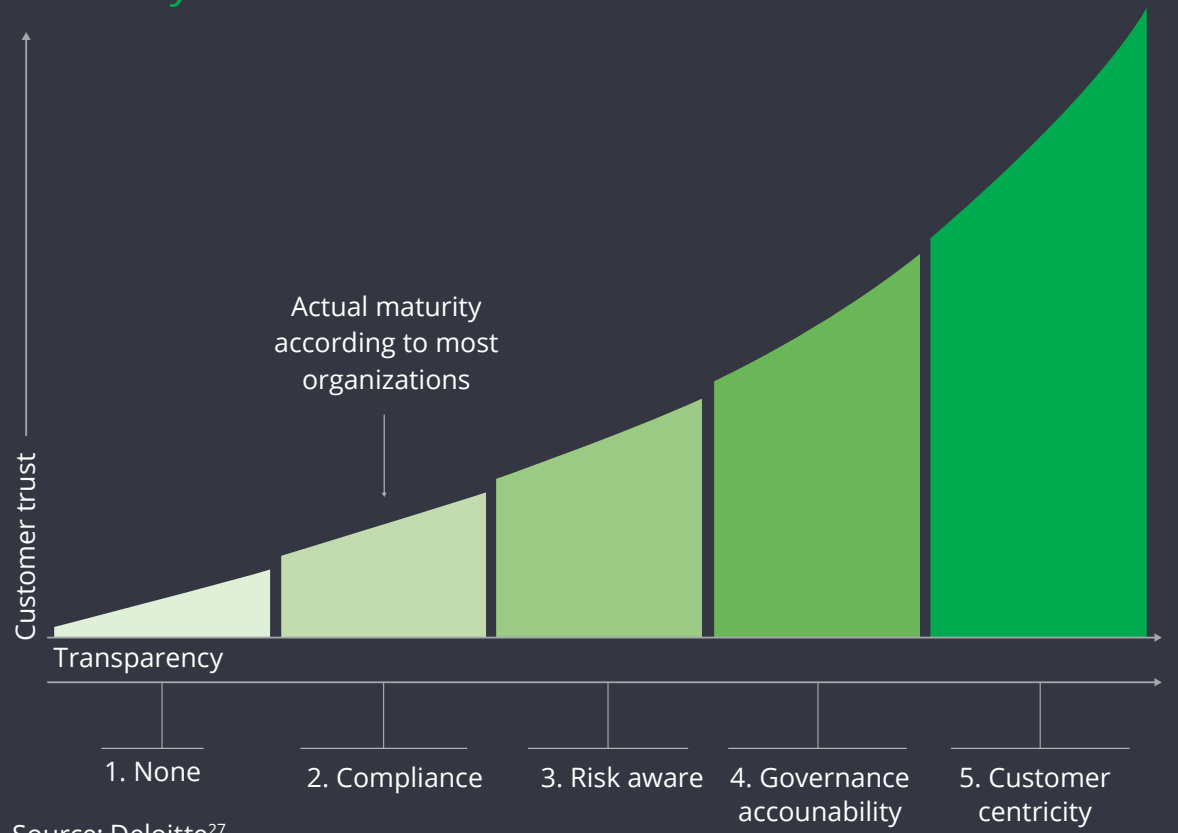
- Virtual crime risks
- Sustained remote-work risks
- M&A and corporate restructuring risks
- Virtualization risks
- New talent model risks
- Trust and data ethics risks

For each of these, be prepared to address the legal implications of cyber risk.

3 Value

Identify the differentiated contributions that enable competitive advantage.

Information privacy and data protection maturity model



Source: Deloitte[27]

? Did you know?

The most frequently cited barrier to managing cybersecurity across the organization is a need for better prioritization of cyber risk, according to C-level executives.[26]

4 Capabilities

Determine existing and in-demand assets and competencies, then identify investments, processes, and technologies to support them.

As a **business advisor,** the CLO is someone who views basic compliance as table stakes and understands relative risk sufficiently to work productively with colleagues and stakeholders internally and externally. One of the most important relationships the CLO should seek to build is with the chief information security officer (CISO). Together, the CLO and CISO can enable the organization to conduct business with risk-based protections.

As the **legal function leader,** the CLO may look to appoint someone—whether internally or from outside counsel—to stay abreast of developments in cybersecurity, both from a proactive regulatory navigation perspective and from a risk and liability perspective. Either way, this resource needs a firm grasp of the company's business operations and appetite for risk, particularly in the context of business continuity and disaster response.

Competencies for a legal function cyber specialist may include:

- Data loss prevention
- Data governance
- Cryptography
- Information classification
- Data mapping and inventories
- Privacy
- Risk-oriented tools and dashboards

The ability to relay often-complex information into everyday lessons can be another valuable skill. The legal function cyber specialist may need to design, facilitate, or support cybersecurity training across all levels of the organization.

4 Capabilities (cont.)

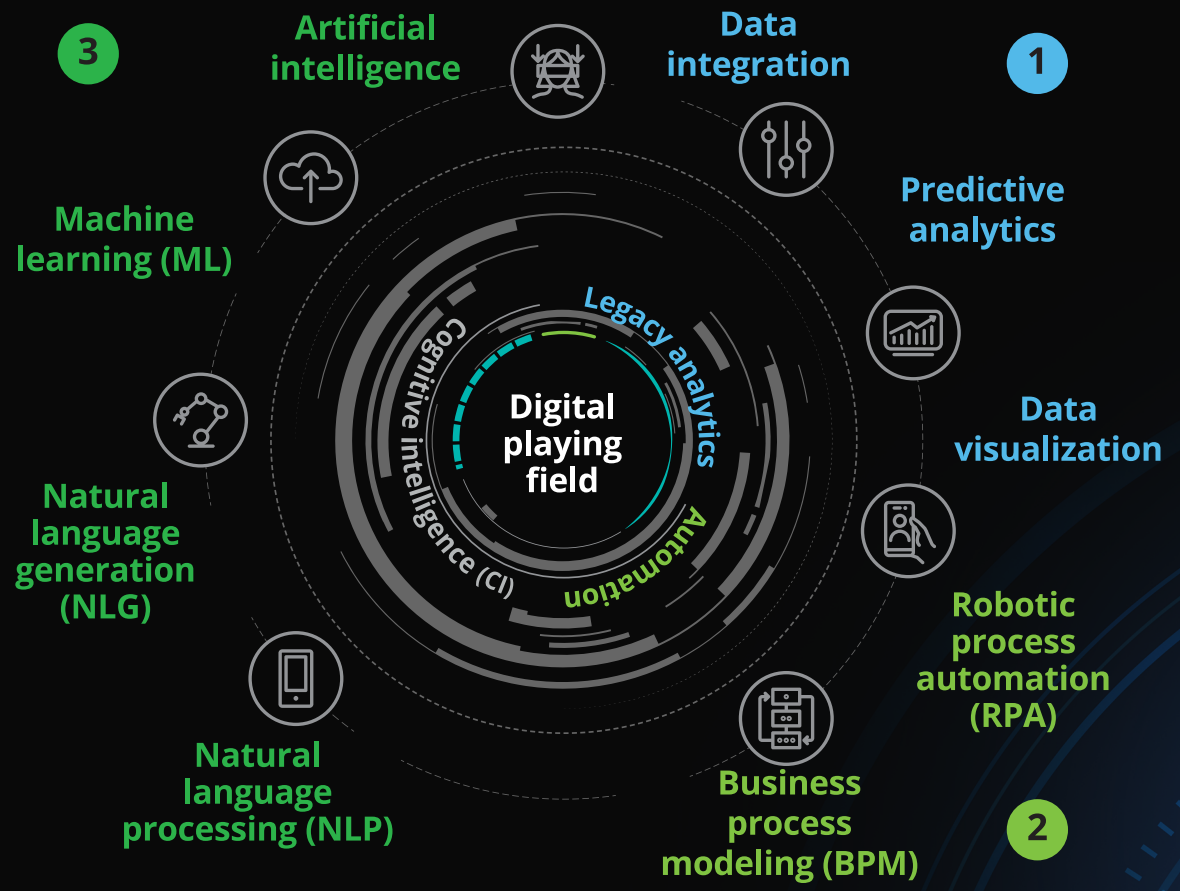
Determine existing and in-demand assets and competencies, then identify investments, processes, and technologies to support them.

Technologies for threat monitoring and prevention

By working with the CISO, the legal function's cyber lead can become familiar with how the organization is:

1. Harnessing data to increase coverage and frequency of measurements and to gain operational insights
2. Adopting process automation to drive scale and accuracy, including in outsourcing
3. Implementing cognitive techniques as data quality and process sustainability warrants

This knowledge can enhance the CLO's credibility as a business advisor on the legal aspects of cybersecurity.



Source: Deloitte[28]

4 Capabilities (cont.)

Determine existing and in-demand assets and competencies, then identify investments, processes, and technologies to support them.

What is zero trust security?

Zero trust security is a technology architecture based on the principle, "Never trust, always verify." It replaces simple verification of entities with real-time access decisions based on continuous risk assessment. The result is a shift from the traditional approach of protecting the perimeter to one where trust is established between individual resources and consumers, as and when required.

What is driving the move to zero trust?

- The rapid pace of digitization is increasing IT complexity and driving up cost.
- An increasingly mobile workforce now expects to be able to work from anywhere, on any device.
- The development of digital products and services shifting toward cloud adoption.
- The demand for better and easier business collaboration and supply chain integration.
- Adversaries are very sophisticated and are outmatching current cyber defenses.

Source: Deloitte[29]

5 Leadership

Consider the culture, talent, training, and behaviors necessary to enable success.

As a **business advisor,** the CLO needs to play in many spaces—both offensive and defensive. This can include:

- Advising on contracting so the organization has more flexibility in data usage
- Helping to manage exposure created through commercial contracts and/or pass that exposure on to responsible third parties
- Identifying and prioritizing risk
- Navigating the evolving regulatory environment
- Planning for and participating in incident response
- Keeping stakeholders and the legal function informed and appropriately trained in cybersecurity issues

Since some of these aren't often exclusively under the legal team's mandate, building influence will be key to helping the organization mature its approach to cybersecurity.

As the **legal function leader,** the CLO can set the example by being cyber-savvy and creating opportunities for the legal team to develop their own knowledge of cyber, especially in the area of law they practice in. Actions to take include providing regular training opportunities and facilitating relationships between legal function leaders and cyber leaders in the organization. CLOs can also encourage the legal team to be ever vigilant, practice cyber breach response, and bring cyber awareness to everything they do.

Putting strategy into action

Because cyber risk is a quickly and constantly evolving threat, strategy—too—must evolve. It's not enough to simply have a strategy. Effective implementation and continuous reevaluation are necessary as well.[30]

To help strengthen the organization's cyber hygiene, legal departments can:

Get the fundamentals right

- Take an active role in privacy and build fraud-prevention controls (expect cyber incidents)
- Continually communicate with and further train employees to take an active role in security
- Stay apprised of and communicate changes in regulatory requirements to stakeholders

Putting strategy into action (cont.)

Set expectations internally and externally

- Frame what the organization will do
- Convey what it expects your customers or partners to do contractually
- Identify and practice incident response

Build toward continuous improvement

- Understand risk
- Identify and prioritize significant risks
- Analyze trends and drive actionable insights
- Actively influence compliance with near-real-time awareness

"The roles of the CLO and CISO, and their relationship with each other, are increasingly important in making organizations more cyber resilient. By joining forces on discovery, communication, and management, these two executives can lay the foundation of an effective cyber strategy and make the case for cyber-related investments at all levels of the organization."

Deborah Golden, Principal,
US Cyber & Strategic Risk Leader,
Deloitte & Touche LLP

Bridging the gap between security and business

The growing frequency and severity of cyberattacks have pushed cybersecurity higher on the agenda of the board and C-suite executives, including the CLO. An effective cyber strategy needn't take the legal team into highly specialized IT territory, but it does require a basic familiarity with the issues and what they mean from a risk and compliance perspective. With that, the CLO can create a multidimensional approach and leverage key relationships to proactive and effective cybersecurity co-owned by leaders across the entire organization.

More in the CLO strategist series:

The CLO strategist: A new kind of legal officer for the modern business

The CLO strategist: Intellectual property

Authors

Lori Lorenzo
Chief Legal Officer Program Research & Insights director
Managing director | Deloitte Risk & Financial Advisory
Deloitte Transactions and Business Analytics LLP
lorilorenzo@deloitte.com

Deborah Golden
US Cyber & Strategic Risk leader
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
debgolden@deloitte.com

Jessica Anderson
US Discovery & Data Management leader
Managing director | Deloitte Risk & Financial Advisory
Deloitte Transactions and Business Analytics LLP
jessicaanderson@deloitte.com

Khalid Kark
US Chief Information Officer Program Research leader
Managing director
Deloitte LLP
kkark@deloitte.com

Sayo Martin
US Cyber & Strategic Risk
Managing director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
saymartin@deloitte.com

Hallie Miller
US Cyber & Strategic Risk
Senior manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
halmiller@deloitte.com

Endnotes

1. Reuters, "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president," February 14, 2021.
2. Emily Mossburg et al., *2021 Future of Cyber Survey*, Deloitte, 2021.
3. Ibid.
4. Emily Mossburg, John Gelinne, and Hector Calzada, *Beneath the surface of a cyberattack: A deeper look at business impacts*, Deloitte, 2016.
5. Lori Lorenzo, "The CLO strategist: A new kind of legal officer for modern business," Deloitte, 2021.
6. Mossburg et al., *2021 Future of Cyber Survey*.
7. Association of Corporate Counsel (ACC), *ACC Chief Legal Officers Survey*, 2020.
8. A.G. Lafley and Roger L. Martin, *Playing to win: How strategy really works* (Brighton, MA: Harvard Business Review Press, 2013).
9. Julie Bernard, Deborah Golden, and Mark Nicholson, *Reshaping the cybersecurity landscape*, Deloitte Insights, 2020.
10. Deloitte, "Board considerations in the wake of SolarWinds," February 8, 2021.
11. Ibid.
12. Ibid.
13. Ibid.
14. Ibid.
15. Deloitte, *A crisis of confidence*, 2016.

Endnotes (cont.)

16. Ibid.
17. Ibid.
18. Ibid.
19. Mossburg et al., *2021 Future of Cyber Survey*.
20. Deloitte, “CLO survey analysis” presentation, October 2020.
21. Scott Ikeda, “Lloyd’s of London: Cyber insurance will not cover cyber attacks attributable to nation-states,” *CPO Magazine*, December 8, 2021.
22. David Ries, *ABA TechReport 2021: Cybersecurity*, *Law Technology Today*, December 22, 2021.
23. John G. Loughnane, “2020 cybersecurity,” American Bar Association, October 19, 2020.
24. Ibid.
25. Ibid.
26. Mossburg et al., *2021 Future of Cyber Survey*.
27. Deloitte, *Deloitte’s Cyber Risk capabilities: Cyber strategy, secure, vigilant, and resilient*, Deloitte, 2017.
28. Deloitte, “Accelerating security imperatives of the future” presentation, November 2020.
29. Mossburg et al., *2021 Future of Cyber Survey*.
30. Deloitte, *Deloitte’s Cyber Risk capabilities*.

Deloitte.