THE **PROVIDENCE** GROUP

Data Risk Warning Intelligence

Using strategic warning methods and tradecraft to reduce risk

Strategic warning intelligence as an approach to managing risk

Strategic warning intelligence, created as a result of the surprise attack on Pearl Harbor in 1941, is an intelligence discipline and methodology that combines multiple sources of information, expert insights, and specialized tradecraft to provide executive decisionmakers advanced knowledge and understanding of strategic risks to prevent or limit damage and to identify opportunities to advance their organization's goals.

Strategic warning is a process of risk communication. Effective warning of risk comprises three elements: it has to appropriately identify relevant contingent risks, it has to be timely and persuasive, and it has to facilitate executive decision making and organizational action. The success of warning is not whether or not all surprises are eliminated, but rather whether the organization appropriately prepared in advance to manage a strategic risk, even if it had been deemed unlikely.

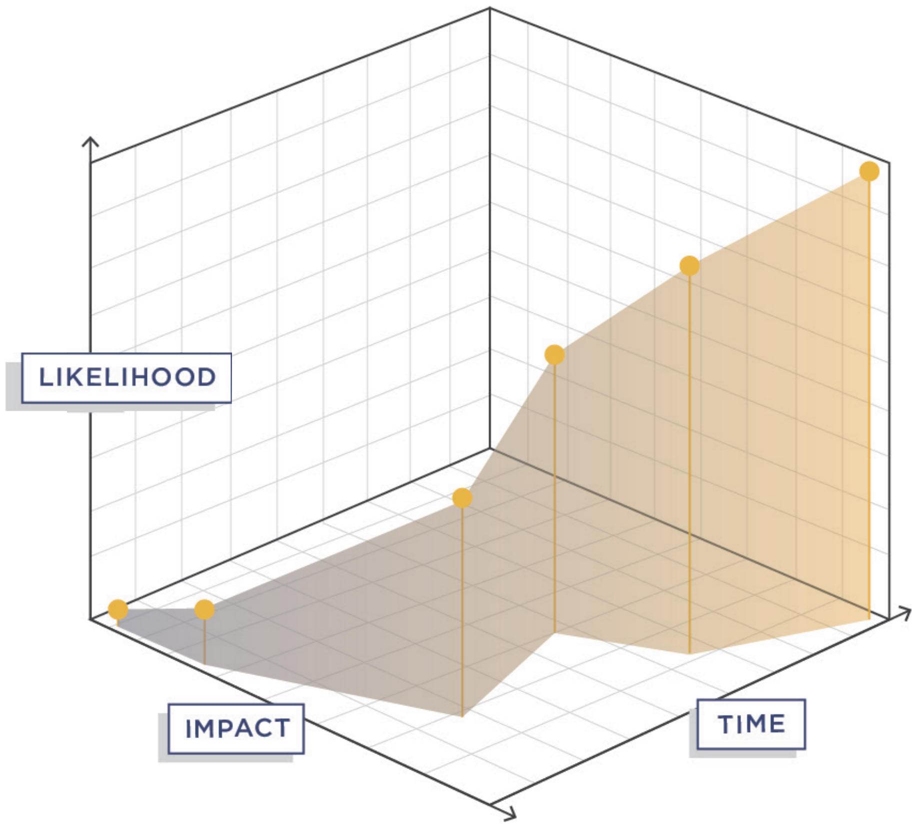
Tradecraft refers to the methods, processes, and techniques used to correctly identify critical risk issues, collect and vet relevant information sources, and produce analytical products that go beyond press reporting to provide insights that enable senior executives to better manage uncertainty.

What is strategic data risk?

Strategic data risks are the threats to an organization's strategy or mission from the malevolent or unintended consequences of cybersecurity events, privacy exposures, or harm resulting from the use or misuse of data. Business executives make decisions on a range of strategic issues, including the future direction of the enterprise, capital investments, mergers and acquisitions, and partnerships. The one thing all of these strategic decisions have in common is that they are reliant on the digital information technology and data that are ubiquitous across enterprise operations. As a result, the collection, storage, sharing, protection, and use of data itself can create strategic risks that manifest across the enterprise and whose impacts are felt through other risk categories, including financial, legal, political, regulatory, reputational, operational, and supply chain/third party.

The Providence Group provides clients with data risk warning intelligence reports that are based on the approaches pioneered by the Office of the National Intelligence Officer for Warning, the National Warning Staff, and the CIA's President's Daily Brief. These include:

- Highly selective warning topics that are tailored to client needs;
- A monthly intelligence report written for senior executives and briefed in person or virtually to provide additional context and for follow up questions and clarifications;
- The opportunity for cross-functional discussions of risks.



The importance of integrating warning intelligence with risk management

The traditional approach to assessing risk is a calculation of the likelihood of the risk in relation to the impact of the risk. The problem with this approach is that it does not take time into account. The US Intelligence Community's Intelligence Advanced Research Projects Activity has demonstrated that over the course of time the integration of additional risk information has markedly improved forecasting future risks through the application of Bayesian thinking to risk problems. What this means is that senior executives are able to update their risk calculations with the addition of new information over time and improve the likelihood that they will make better risk calculations.

01000100011101010010100010101010101001100011111010101010110
0101010100101000101011101010010101000101001010001111010101000
1000100010001000101010011110011101010100010001110101000
101000101010101010100110001111101010101010010010101001010001010111010

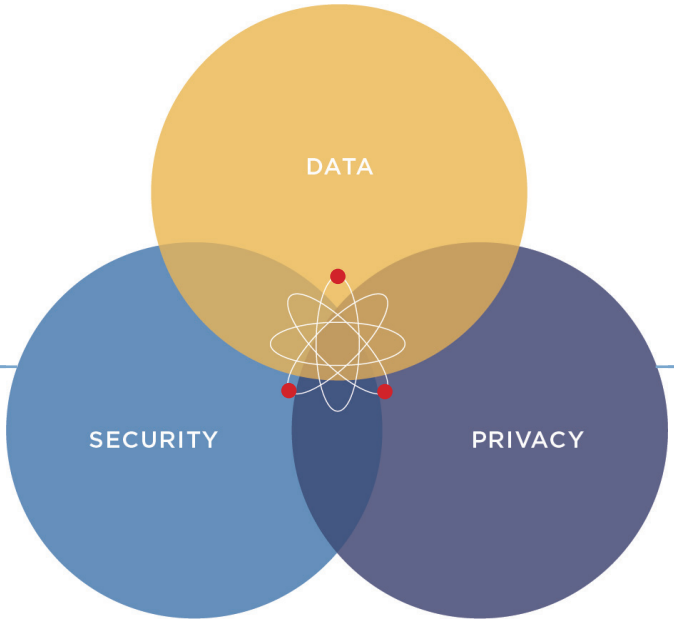
Risk warning intelligence reports support this approach to better risk decision-making by providing senior executives relevant information about strategic risk problems in a focused and time efficient manner.

Time is the most important commodity for senior executives, and it is not practical, let alone possible, for senior decisionmakers to stay current with all of the information across the 12 different strategic data risk areas. Risk warning reports ensure that senior executives are aware of the most important developments in data risk in easy to digest narratives and briefings and are updated on these risks over time.

The value of early warning

Risk is uncertainty about the future. Having early warning about risks provides decisionmakers an advantage when having to make strategic decisions. Integrating risk warning intelligence into an organization's risk management process also provides additional value-added benefits:

- The earlier a risk can be identified and managed the less it costs;
- Discussion of future risks across functional teams leads to more efficient solutions for risk mitigation;
- The early warning of risks can also lead to the identification of opportunities to further organizational strategy and goals.



Strategic data risks are contingent and must be viewed in context

Assessing the risks data pose to an organization is made all the more difficult by the contingent and dynamic nature of the data itself. Often, data risk is represented by a Venn diagram that shows the relationship between privacy and security. This representation accurately shows that cybersecurity and privacy are both distinct and overlapping, yet it unintentionally obscures a lot of risk many organizations face.

A better representation of the complexity of data begins with a three-circle Venn diagram that includes security and privacy, but also adds data use to recognize the risks that are associated with using data, such as industrial data that can have competitive advantages that must be protected or certain health or financial data that has potentially harmful impacts.

Overlaying the Venn diagram are individual datum that orbit the diagram and crossover each of the circles and through their overlapping areas. This part of the diagram captures the contingent aspect of data and the determination of whether or not data will pose a risk is based upon the context of where those data reside at any given moment.

An example of this is the near instantaneous movement of non-public forward looking financial information from being highly secured private information in the context of protecting against insider trading to publicly reported information through the Securities and Exchange Commission to appropriately inform investors.

It is the context in which the data resides that determines the degree to which there is data risk. Static risk appraisals that view data in binary compliance terms—it is privacy information or it is not?—will often obscure strategic risk because it fails to take into account the future that could alter the context of the risk.

CASE STUDY

Business email compromise (BEC) attack warnings

Risk challenge

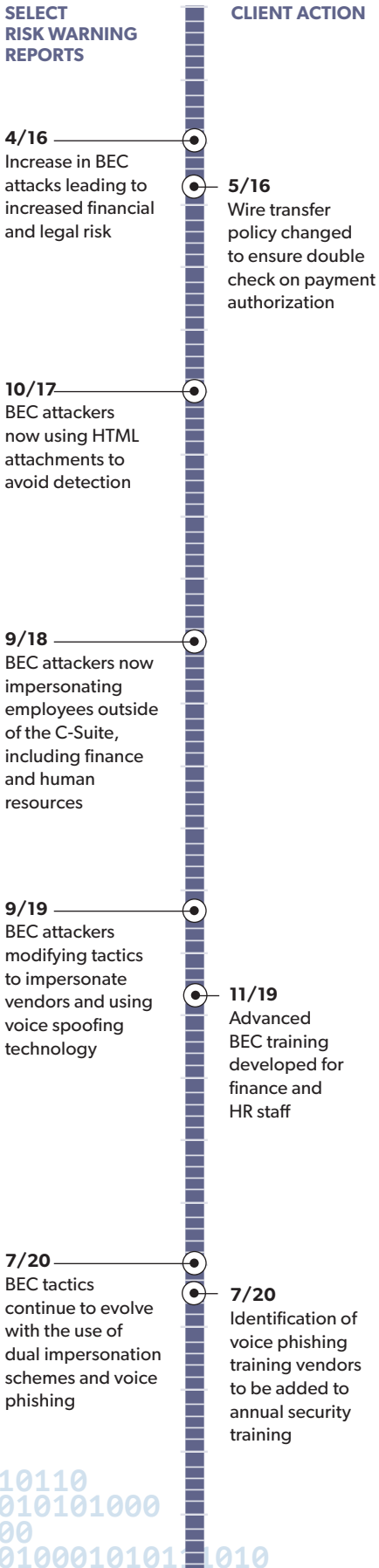
A multibillion-dollar organization that has more than a thousand vendors is a frequent target of BEC attacks that could cause financial, legal, and reputational risks if the attacks are successful. The organization has no internal capacity to monitor the often changing and increasingly sophisticated tactics used by criminal organizations in order to mitigate this risk.

Warning communication

Over a five-year period we provided seven BEC specific risk warning reports that traced the increase in the scale and scope of the BEC threat as well as specific actionable warnings on the changes in BEC tactics.

Warning impact

As a result of our first BEC warning report the client changed their internal process for wire transfers to include a telephonic confirmation of the authenticity of the request. This change in protocol led immediately to the thwarting of a first BEC attack at the organization. The client has subsequently been able to modify their security posture against BEC attacks by instituting low-cost mitigation strategies as BEC tactics have changed.



CASE STUDY

New state level regulatory risk warning

Risk challenge

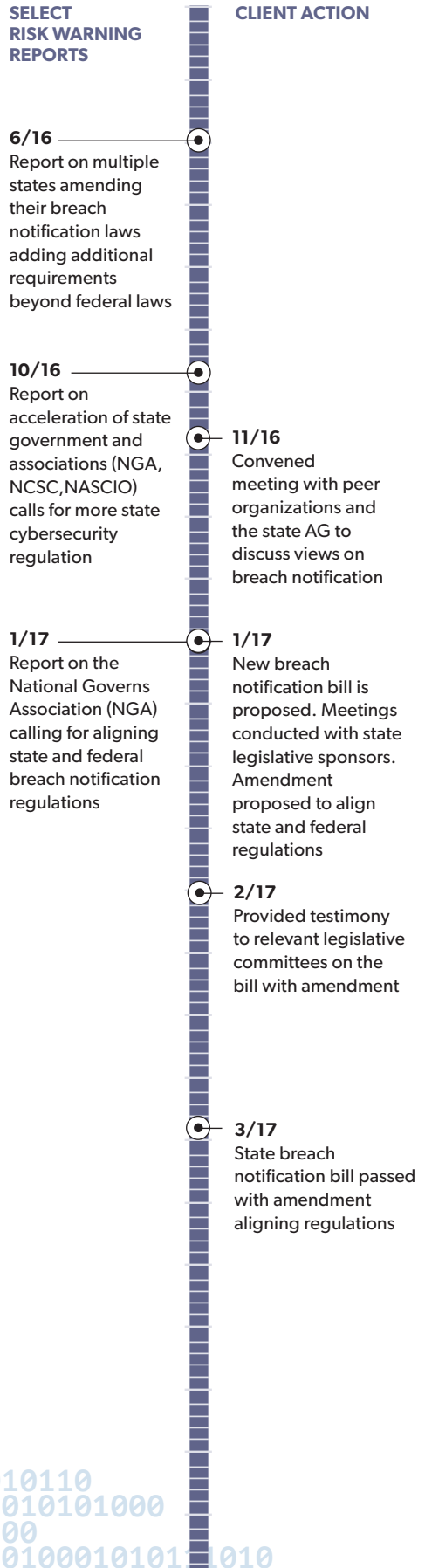
A highly regulated multibillion dollar organization maintains an elaborate and expensive federal compliance program. Additional federal regulations or new state-specific laws would require new investments in the compliance program and increase regulatory risk.

Warning communication

We produced three risk warning reports over the course of eight months that described an increasing movement at the state level to introduce new legislation that would create new or amend existing cybersecurity and privacy regulations. Within weeks of our third risk warning report, a bill was introduced in the state legislature to amend the state's breach notification bill that would impose compliance requirements that did not align with the required federal regulations.

Warning impact

The client did not have a process to identify future regulatory risk and coordinate risk management activities across functional areas within the organization. The risk warning reports were circulated among the executive team, including the CEO, CIO, General Counsel, and the government affairs office, to develop a common understanding of the potential risk and to coordinate a risk mitigation strategy. The client, using the information in the reports, was able to create a coalition of leading peer institutions, meet with the state Attorney General, the bill's legislative sponsors, and provide testimony in support of an amendment to the bill that aligned the state requirements with current federal regulations. The amended bill was signed into law.



CASE STUDY

Anticipating new cybersecurity requirements for federal research funding

Risk challenge

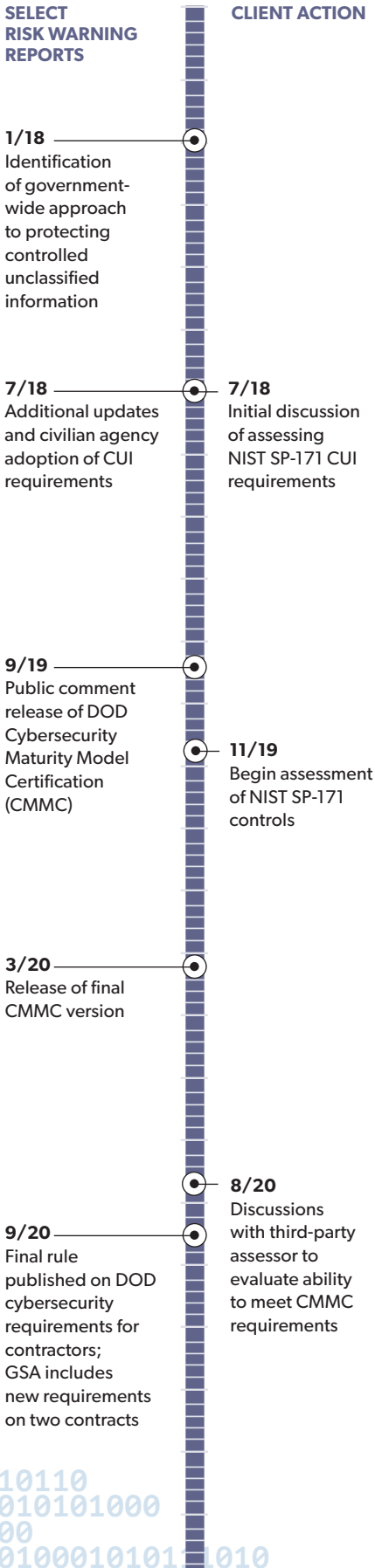
A large academically affiliated medical system maintains elaborate and expensive federal compliance programs to meet Department of Health and Human Services (HHS) regulations, including HIPAA, that also meet the cybersecurity and privacy criteria for federal research funding from defense and civilian agencies. New cybersecurity requirements for federal funding outside of HHS's traditional approach pose financial, operational, reputational, and compliance risks.

Warning communication

We provided warning reports for nearly two years about the possibility of new cybersecurity requirements regarding a category of information produced by the federal government and by government funded contracts called "controlled unclassified information" (CUI). We identified that CUI was increasingly being adopted by non-defense agencies and might impact other government funding vehicles. We delivered a series of five warning reports that provided early warning of this new regulatory requirement.

Warning impact

The client was not aware of the activities surrounding CUI at either the National Institute for Standards and Technology or at the Department of Defense (DOD). The warning reports contributed to an understanding of CUI and the likely regulatory requirements for future DOD funding vehicles. The warning reports also provided advanced knowledge of the potential civilian agency use of CUI and the DOD regulatory construct for other funding vehicles that might impact the client.



About The Providence Group

The Providence Group helps organizations navigate the complexity of data risk in order to thrive in today's uncertain environment through the use of national security and intelligence methods and tradecraft. Our approach to risk management empowers executives and builds value through deep organizational insights, foresight of unanticipated risks, and organizational capacity building.

THE **PROVIDENCE** GROUP

1440 G Street NW
Washington, DC 20005

Phone: (202) 922-5515
info@providencegroupdc.com