Essential Assumptions for Effective Data Security

亦有中文简体译本
www.isaca.org/currentissue

The biggest challenge facing data security functions and the organizations relying on them is not a technology problem or even the looming threat of cyberattack. Rather, it is making sure that everyone in the organization is on the same page and basing their decisions and actions on the same set of assumptions.

According to research by Enterprise Management Associates (EMA), many organizations have regional or divisional plans for security operations that can result in wasted resources and slower incident response times, among other problems.[1] Particularly in organizations where the data security function is expected to run in the background and keep things safe, it is likely that there are differing priorities, expectations and assumptions concerning the relationship of data security to business management, technology and other areas.

For data security efforts to be effective, it is critical that people in all areas and levels of the enterprise operate under five key data security-related assumptions. Internal audit should play a key role in this. With its cross-departmental reach and visibility into organizationwide risk management efforts, internal audit is uniquely positioned to promote the necessary alignment and assess whether it is happening.

1. Data Security Teams Should Take an Integrative Approach

Nearly every key aspect of data security is broadening in some way. The definition of the workplace, the location of the workforce, the array of business processes that are data-enabled and the volume of end-user devices have all expanded in recent years. All signs point to the need to take a more expansive, higher-level and more integrated approach to information and data security, as opposed to regarding it merely as a specialized concern.

It follows that many enterprise leaders maintain that their biggest data security challenge is not tactical. Instead, they say, it is the big picture. In a 2021 research survey, respondents were asked, "What is your organization's greatest data security problem/challenge?" The top-two responses were:

1. Unified security strategy across entire organization (22.1 percent)
2. Data complexity/complexity of data deployments (16.2 percent)[2]

A dedicated data security team with defined responsibilities and accountabilities is a must, but if senior management and the board are serious about developing a unified data security strategy, then the data security team must be asked (and permitted) to work in a more interactive and integrative way

KEVIN M. ALVERO | CISA, CDPSE, CFE

Is senior vice president of internal audit, compliance and governance at Nielsen Company. He leads the internal quality audit program and industry compliance initiatives, spanning the enterprise's Global Media products and services.

BRIAN ALVERO | CAL, CSM, CSP, CSPO, CSSBB

Is the chief information officer and chief security officer at the Pasco County, Florida, USA, Sheriff's Office. He leads the overall technology solutions, initiatives and strategies for the entire agency.

across all areas of the organization. This includes having upstream interactions with strategic planning, product development and customer service teams, for example, to ensure that data protection is a forethought for them rather than an afterthought.

This approach helps not only to minimize data security vulnerabilities, but also to maximize efficiency. In organizations without a unified strategy, there is greater likelihood of wasting money on tools that are redundant or are not compatible across multiple areas of the organization. As noted in the most recent *Microsoft Digital Defense Report*:

> *Organizations must be able to see across their apps, endpoints, network, and users…[they] will also be driven to reduce costs by adopting more of the security capabilities built into their cloud and productivity platforms of choice. To maximize the effectiveness of security organizations, tools must be fully integrated to improve efficacy and provide end-to-end visibility.*[3]

How Internal Audit Can Help

Internal audit is uniquely positioned to look across the entire organization and determine where there are misalignments and redundancies between different areas of the business. Although a discreet data security audit may be useful, internal audit may serve better to integrate data security into each audit it conducts to build a sense of alignment over time.

2. Data Privacy Programs Can Create Competitive Differentiation

At many organizations, data security teams have a role similar to sports officials; they are regarded as doing their best work when they are unperceivable and receive attention only when something goes wrong. However, the data security function and the people who execute it are increasingly coming to the forefront. *CSO* reported that nearly half of organizations surveyed were increasing cybersecurity spending in 2022, with nearly all at least keeping it level.[4] Meanwhile, more organizations are deciding that if they are going to spend vast amounts of money on data security and regulatory compliance, then they should be able to use it to proactively tell their customers a compelling story. In the aforementioned survey, more than 70 percent of respondents indicated they could use—or already had used—their regulatory compliance or data privacy programs as a competitive differentiator in the marketplace.[5]

With the EU General Data Protection Regulation (GDPR) and the US State of California Consumer Privacy Act (CCPA) leading the way, data privacy regulation is likely to expand considerably in the coming years, and organizations must look at consumer skepticism and the more aggressive regulatory environment as presenting opportunities. Those that continue to approach privacy regulations solely as a constraint are going to get squeezed tighter and tighter. To seize opportunities, organizations must get better at communicating with their customers, both collectively and individually, about data security and the trust-value relationship, thus encouraging customers to willingly exchange information for value because third-party tracking data are going to become increasingly harder to obtain.

To seize opportunities, organizations must get better at communicating with their customers, both collectively and individually, about data security and the trust-value relationship.

A recent McKinsey and Company report states, "The issue with many corporate data-privacy initiatives, is that they are too technical or legalistic for the everyday customer." To create a successful data relationship, according to the report, enterprises should consider investing in a full-time data relationship manager.[6]

Having a person with strong communication skills, complemented by technological expertise, would enable organizations to guide their customers to understanding data protection policies and technologies in a way that focuses on value, as opposed to wading through terms of use and perfunctorily clicking "Accept."

The McKinsey report further states,

> *Companies that invest in these elements of data relationship management have an opportunity to take a leadership position around data protection that could pay dividends in the years to come.*[7]

LOOKING FOR MORE?

- Read *Zero Trust: How to Beat Adversaries at Their Own Game. www.isaca.org/zero-trust*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Organizations also need to do a better job communicating to their own people. Offering security awareness training programs is a common practice, but some employees still cling to the misperception that data security policies and personnel mainly prevent them from doing things they need to do (necessitating workarounds) or catch them doing things they are not supposed to do. As with customers, proactive messaging to employees around compliance should be value-driven and focused on how the data security team can enable the organization and its employees to succeed, rather than merely to control risk.

How Internal Audit Can Help

Internal audit is on a similar journey, from an image perspective, and can help to evaluate whether communication efforts are understandable and value-based, and whether they present a positive image of the data security mission.

3. Zero Trust Is the Path Forward

The traditional trust, but verify approach to network security automatically trusts users and endpoints within the organization's perimeter, putting the organization at risk from malicious internal actors and making legitimate credentials vulnerable to takeover by malicious actors.[8] As the dispersal of the workforce continues, along with increasing cyberattacks, a zero trust approach to authenticating users should be the paradigm that every organization is working under or toward.

According to the *Microsoft Digital Defense Report*, multifactor authentication (MFA), a key component of a zero trust framework, prevents 99 percent of unauthorized access due to credential theft. The report states, "This means that right now, every one of us is on a Zero Trust journey—whether we know it or not."[9]

How Internal Audit Can Help

Internal audit is a key partner with data security in understanding the effectiveness of organizational controls and identifying potential vulnerabilities in a zero trust environment.

4. Incident Response Is Just as Important as Incident Avoidance

In the Disaster Recovery Institute's *Seventh Annual Global Risk and Resilience Trends Report*,[10] the three threats survey respondents ranked highest overall in terms of the business impact to their organization were cyberattacks, IT outages and data theft. They made their selections from a list of 20 potential threats that included pandemic, natural disaster, supply chain disruption and climate change.

Incident response must be treated with the same diligence and sense of urgency as incident avoidance.

Meanwhile, the steadily increasing number of global weekly cyberattacks hit an all-time high of 925 attempts per organization in the fourth quarter (Q4) of 2021.[11] It has become a common refrain among security experts that every organization, sooner or later, will be the target of a cyberattack.

If risk is indeed a function of likelihood and impact, then cybersecurity resilience clearly should be a high priority for every organization. Incident response must be treated with the same diligence and sense of urgency as incident avoidance. It should involve not only documented plans, but also regularly rehearsed and reinforced behaviors designed to bring about quick and appropriate action in the critical moments after a breach or attempted attack is detected.

How Internal Audit Can Help

Internal audit can help by raising awareness of attack frequency and vulnerability trends and by including cybersecurity incident response planning in the internal audit program. In addition, internal audit can help connect cybersecurity risk to business impact in a way that is compelling for business leadership.

5. When It Comes to Data, More Is Not Necessarily Better

Due to the lure of the unlimited possibilities of big data-enabled applications, organizations have been trained to look at their data as a key strategic asset, and rightly so. At the same time, considering the potential legal, financial and reputational damage represented by a data breach, data security professionals and the enterprises they serve must also be mindful of the potential liability associated with organizational data—and the stakes are going up.

Compliance Week reported that nearly US$1.2 billion in fines were issued against organizations in 2021 for violations of GDPR.[12]

Meanwhile, in January 2022, the European Data Protection Supervisor (EDPS) notified EU law enforcement agency Europol of an order to delete data concerning individuals with no established link to a criminal activity. This was one highly publicized instance of an organization being cited for possessing data that regulators believed it should not have possessed.[13]

In short, it is not always better to have more data. Instead, the keep or do not keep decision has to come down to the value of the data, given the risk of a breach.

How Internal Audit Can Help

Internal audit can ensure that robust data retention policies exist and verify through qualitative and quantitative audit techniques whether they are understood and followed. It is also important for internal audit to communicate the business risk of failing to make good data retention decisions to justify the audit effort.

Conclusion

The most sophisticated technical solutions to today's cybersecurity issues can be rendered useless if an organization's people are not aware and aligned when it comes to understanding its larger data security strategy and their role in pursuing it. Disparate assumptions and expectations across the organization can undermine even a highly skilled and well-funded data security force. Top management would, therefore, be wise to invest in communication efforts to ensure that critical assumptions are pervasive throughout the organization. Internal audit can help achieve that unified perspective.

Endnotes

[1] Steffen, C. M.; *Data Security in a Multi-Cloud World*, Enterprise Management Associates (EMA), USA, 11 August 2021, *https://www.ibm.com/downloads/cas/6EODENGR*

[2] *Ibid*.

[3] Microsoft, *Microsoft Digital Defense Report,* USA, October 2021, *https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi*

[4] Pratt, M. K.; "Cybersecurity Spending Trends for 2022: Investing in the Future," *CSO*, 20 December 2021, *https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html*

[5] *Op cit* Steffen

[6] Brodherson, M.; A. Broitman; J. Cherok; K. Robinson; "A Customer-Centric Approach to Marketing in a Privacy-First World," McKinsey and Company, 20 May 2021, *https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/a-customer-centric-approach-to-marketing-in-a-privacy-first-world*

[7] *Ibid*.

[8] Raina, K.; "Principles of the Zero Trust Model," Crowdstrike, 6 May 2021, *https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/*

[9] *Op cit* Microsoft

[10] Disaster Recovery Institute International Future Vision Committee, *Seventh Annual Global Risk and Resilience Trends Repor*t, USA, 2021, *https://drii.org/crm/presentationlibrary?plsharekey=346cbc8d7c96e8c*

[11] Muncaster, P.; "Corporate Cyber-Attacks Spike 50% in 2021," *Infosecurity Magazine*, 11 January 2022, *https://www.infosecurity-magazine.com/news/corporate-cyberattacks-spike-50/*

[12] Hodge, N.; "Report: GDPR Fines Surpass $1B in 2021; Breach Notifications Also Rise," *Compliance Week,* 18 January 2022, *https://www.complianceweek.com/regulatory-enforcement/report-gdpr-fines-surpass-1b-in-2021-breach-notifications-also-rise/31259.article*

[13] European Data Protection Supervisor, "EDPS Orders Europol to Erase Data Concerning Individuals With No Established Link to a Criminal Activity," 10 January 2022, *https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en*