COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2021
Engage with business leaders to mitigate pandemic-induced security risk

By Ralph Villanueva, CISA, CISM, PCIP, ITIL, CIA, CRMA, CFE

Ralph Villanueva (rvsvillanueva@yahoo.com) is IT Security and Compliance Analyst for Diamond Resorts International in Las Vegas, Nevada, USA.

On a chilly Las Vegas evening in March 2020, I received an urgent call from the manager of a conference for which I was a speaker. "Conference plans have drastically changed, and you need to deliver your presentation tomorrow. All nonessential businesses in Nevada are closing on March 17 to contain the rapid spread of the pandemic." A few days later, the eternally neon-bright Entertainment Capital of the World went dark—literally.

The COVID-19 pandemic emptied corporate offices around the world. Working from home became the new norm, and major tech companies such as Twitter, Google, and Microsoft[1] even told their employees they can work away from the office for as long as they need to. A lot of office denizens who are adept with technology and are comfortable working in pajamas welcomed this good news.

However, this feeling was not often shared by a key member of the compliance function. The information technology (IT) compliance professional, who is responsible for compliance with the IT aspects of statutory, regulatory, and legal requirements, also faces several technology-enabled challenges and threats that a work-from-home scenario poses to a typical corporation's information system. Consider some of the recent security threats and challenges faced by IT leaders during the COVID-19 pandemic:

- Increase in cyberattacks such as data leaks, business email compromise, and phishing campaigns[2]
- Increased insider theft of sensitive financial and personally identifiable information[3]
- Employee information security risks[4]

Though these seem to be complex technology-enabled problems, the IT compliance professional in particular and the compliance profession in general can play a greater role and add more value to the organization than ever before. The simple reality is that technology is but an enabler of the overall business strategy. The compliance function is the bridge that connects the business deliverables to the compliance requirements, which in turn keep the company in line with its strategy for fulfilling its growth and profit objectives. It also keeps the company safe from legal or reputational risk brought about by noncompliance to mandatory statutory, regulatory, contractual, or legal requirements. So what are the ways by which IT compliance and the overall compliance department can work together to mitigate information security incidents?

The people, process, and technology approach

IT audit and compliance practitioners can classify IT issues that lead to information security incidents into three components: people, process, and technology (PPT). Like a three-legged stool, each of these elements is equally important to the overall stability of the entire IT system. The IT compliance professional, in coordination with the general compliance and IT departments and the business owner, can then work on solutions according to

each component in the PPT approach.

Take data breaches. Studies have shown that social engineering is a major culprit that enables cybercriminals to initiate data leaks, business email compromises, and successful phishing email attacks. Social engineering is a broad term used to describe various ways by which computer users are tricked to do the hacker's bidding, such as phishing emails, which fool computer users into clicking on a link or downloading a file. The users inadvertently download a malicious software, which enables the thieves to raid the company's database of everything from intellectual property to sensitive customer information. These criminals can also plant ransomware and brick up access to company databases and applications until the company pays a ransom.

By applying the PPT approach here and starting with a focus on the "people" component, the IT compliance professional can assess the extent to which computer users are trained in recognizing social engineering attacks and how to avoid them. The compliance professional can then look into the manner by which IT support staff provide computer users with certain access rights (i.e., the "process" component). Are staff-level users who do not perform administrative functions in certain applications given privileged administrative rights? If so, this provides the cyberattacker with a wider exploitable attack vector or surface. Moreover, certain emails that are social engineering attempts from a blacklisted source can be blocked by the IT system's firewalls (i.e., the "technology" component).

The same three-component approach applies to mitigating insider attacks as well. Constant supervision and proactive management will more likely dissuade would-be insider criminals from stealing valuable company data and assets (people component). A vetting process that includes a criminal background check is more likely to prevent repeat criminal offenders from ending up in your company's IT department (process component). Additionally, a robust set of computer access controls will drastically reduce the chances of an employee in lower management viewing and downloading sensitive company information (technology component).

A final example focuses on the work-from-home environment. A lot of remote employees use the company laptop for noncompany activities like children's school work, gaming, and shopping, as well as for video conferencing applications, which may not be on par with their company's enterprise security standards. This exposes the company to a single point of failure, which is the employee who does not observe proper information security practices.

A combination of continuous information security training (people component), proper user access provisioning (process component), and removal of administrative rights to the company laptop (technology component) can catch a lot of these security lapses in a remote work environment. Also, a lot of information-security-conscious companies limit administrative rights to user laptops to a few IT technical support staff who log in remotely to fix or install company-approved applications. This prevents the user from installing unauthorized applications or modifying the malware setting of the company-issued computer.

Engaging with business process owners

The next part of this process is to ask how the business process owners can help the IT compliance department enforce all relevant IT regulatory, statutory, and legal requirements. The proliferation of data privacy regulations such as the General Data Protection Regulation and the California Consumer Privacy Act, the stringent medical information privacy requirements of the Health Insurance Portability and Accountability Act, and the IT security requirements of the National Institute of Standards and Technology's Special Publication 800-53 for US government contractors are loud reminders that IT compliance is not only the responsibility of the IT compliance professional but is a company-wide responsibility spearheaded by general compliance.

Business process owners are not only the frontline management officers and staff, but can also be the

departments responsible for enforcing various aspects of the compliance requirements that the company is required to follow. For instance, the legal department is a business process owner as far as ensuring that the IT aspects of data privacy and contractual requirements are followed. The risk and safety department is responsible for authorizing access to company premises and managing the electronic ID system that is also under the purview of the IT compliance professional. Collectively, these business owners and departments can deploy a wide array of actions in support of IT compliance, from advocating for strong IT controls and practices to enlisting the support of both key executives and frontline management in enforcing IT security control requirements. At the same time, they can provide feedback from all the levels and departments of the organization to the IT compliance professional as to which IT security controls are working and those that need to be adapted to the unique needs of a department.

Moving forward with defenses ready

The IT compliance professional alone cannot mitigate pandemic-induced information security incidents. However, by using the PPT approach; a combination of strong yet workable IT controls; proactive enforcement and collaboration by IT compliance, business owners, and various departments regarding compliance of applicable IT control requirements; robust support from business process owners; and constant feedback from both senior executives and employees on the front lines, the cybersecurity threats that have multiplied as people work from home can be mitigated effectively.

Takeaways

- Information technology (IT) compliance is a key component in keeping the organization safe from adverse legal and financial issues, and also in achieving growth and profit targets.
- Distill IT compliance issues into three components—people, process, and technology—to simplify analysis and narrow focus on pressing IT compliance issues.
- Closely work with the business or process owners, because their in-depth knowledge of their business or process can make IT compliance recommendations more actionable.
- Work with other members of the compliance function within your organization, such as legal, risk, etc. Some aspects of their function may intersect with IT.
- IT compliance is everyone's business. A chain is only as strong as its weakest link.

1 Kari Paul, "Twitter announces employees will be allowed to work from home 'forever,'" *The Guardian*, May 12, 2020, https://bit.ly/2JFuyaF.
2 Lance Whitney, "How IT leaders were unprepared for the security challenges posed by COVID-19," Tech Republic, July 29, 2020, https://tek.io/3g1hXLg.
3 Sue Poremba, "Remote Insider Data Theft Worries Financial Industry," Security Boulevard, November 2, 2020, https://bit.ly/33COanc.
4 James Coker, "Employee Work from Home Habits a Security Risk to Businesses," *Infosecurity Magazine*, June 3, 2020, https://bit.ly/33zqNe6.