Infosys® | CONSULTING

CYBERSECURITY IN THE COVID-19 ERA

How to manage cybersecurity risks in a post-pandemic world

An Infosys Consulting Perspective
by Andrew Duncan

consulting@infosys.com | InfosysConsultingInsights.com

A FUNDAMENTALLY HUMAN PROBLEM

Malicious actors are already exploiting the uncertainty and disruption caused by Covid-19. Large scale adoption of collaboration tools and conferencing systems have increased risks to cyber threats; security controls may not be applied to hastily implemented new systems, and best-practice procedures could be side-stepped by employees as they adjust to life working remotely.

Right now, organizations must maintain business continuity while adjusting and scaling up security programs to protect against new cyber threats. This will be a difficult balancing act, and is made even harder by the cutting of security expenditure and IT budget freezes that may be necessary to survive the economic downturn.

However, even in the midst of Covid-19, cybersecurity remains a fundamentally human problem; the person at the screen or keyboard is always the weakest point in any technical system. Just as we have reduced the risk of coronavirus through social distancing measures, we will need to develop good security habits to reduce cybersecurity risks.

In this three-part series on cybersecurity, we look at why changing organizational culture has never been more important in preventing cybersecurity breaches than it is right now.

PART I: ORGANIZATIONAL CULTURE AND AWARENESS IS KEY TO CYBER PREVENTION IN 2020

Most of us have heard the quote about cyber breaches, “There are two kinds of companies — those who know they’ve been breached and those who don’t.” And while this line is quickly moving into the realm of cliché, its core message unfortunately rings truer than we’d all wish. What’s also true is that, despite the fact most CEOs and Boards are now meaningfully ramping up investment in cybersecurity, the frequency and severity of attacks will continue to increase post-pandemic.

To best equip businesses to operate in this environment of elevated risk, it is helpful to first create awareness around what one means by a breach.

Cybersecurity incidents are often thought of monolithically, but at Infosys Consulting we find it instructive to view breaches through the lens of the different things bad actors are attempting to accomplish. Often, this is one of two things: stealing information or extorting money. Understanding how each of these could play out at your organization has meaningful implications to both upstream prevention and downstream consequences.

Information theft can come in various forms, but generally entails either the acquisition of personal (e.g. credit card data) or competitive data (e.g. engineering designs). In these breaches, bad actors often gain access to a network and quietly lurk, acquiring data over

a long period of time in the form of hijacked email communications or batch data downloads.

Naturally, the companies most at risk of these attacks are those storing competitive or personal data, with medical and financial data topping the list. With that said, many companies underestimate their risk level relative to these incidents. Information that most firms possess, such as employee passwords and SSNs, are valuable to bad actors who can monetize this information on the deep and dark web.

The second attack objective – extorting money – has become something of a favored pastime among groups such as the Russian mafia. In these scenarios, attackers gain access to the network, encrypt operational data (e.g. databases, app servers, file servers) and, when possible, delete all backups. They then contact the company with a ransom note and a demand to be paid in bitcoin in exchange for a decryption key, a demand most businesses comply with.

Unfortunately, the list of companies this risk vector applies to is exhaustive – it's a rare business indeed that does not run on a foundation of software applications today and even more so with the shift to remote working. And because this has proven to be a profitable business for organized crime, the level of sophistication of these groups continues to rapidly improve.

Step one to counteracting these threats is awareness: companies need to acknowledge that they're at risk and that everyone who works at a company is a potential threat vector. Because of this, everyone at companies should play an active role in breach prevention.

PART II: A CEO MANDATE FOR BASIC CYBERSECURITY HYGIENE

In my last post on cybersecurity, I explored the two primary objectives of cyber hackers: information theft and the extortion of money. What is interesting about both of these goals is that they start in similar ways. Bad actors either find a vulnerable technology via an external technology scan that they use to penetrate a company's network, or they leverage human-centric tactics, such as phishing, to open the front door.

What is surprising to many executives is that, while cyber risk is often thought of more in terms of technology vulnerabilities, it is often the human dimension that leads to breaches. And the individuals most often at fault, partially because they're also the most targeted, are the c-suite executives themselves.

To reduce the risk of security incidents, CEOs should first ensure their businesses are both prescribing, and, more importantly, adopting basic cybersecurity hygiene:

- Multi-factor authentication (MFA)
- Ongoing phishing training

- Strict adherence to patching

These three things, which are both simple and inexpensive, are far and away the most important actions companies can take to protect themselves. Regrettably, because some of them (e.g. multi-factor authentication) can sometimes be viewed as a nuisance to time-strapped employees, these are often deterrents that suffer from partial adoption.

Fortunately, the tools available to drive these security deterrents have continued to improve, making them less onerous to both administer and use. As an example, a number of phishing training businesses have emerged that can automatically increase the level of sophistication of simulated attacks each month to progressively raise the level of maturity within organizations.

Beyond basic hygiene, there are a deeper set of practices and tools firms should implement, including:

- Annual pen tests
- Monitoring tools to scan systems for breaches
- Table-top exercises to prepare for incident response
- External vulnerability scans to identify at-risk technology

From a staffing perspective, the model I have seen work best, through my personal advisory work with large organizations, is to have a named, dedicated CSO (Chief Security Officer) who leverages a combination of in-house and third-party resources and service providers. This combination enables companies to benefit from the expertise of specialists while keeping a healthy degree of ownership inside the business, something I view as critically important.

Even with the right staffing model and tools, however, it's worth reiterating that people, not technology, are often at the heart of breaches. And the common denominator of many of the incidents we've supported clients on has been cultural – firms either failed to take risks seriously or acted as if cybersecurity was solely the responsibility of IT instead of fully integrating the topic within the business.

Looking to the future post-pandemic, it is helpful to remember that culture is shaped by executive action. For this reason, it is vital for cybersecurity to be included in both the dialogue and actions of C-level executives, providing a natural way for employees to understand that security is a company priority.

PART III: MANAGING INCIDENT RESPONSE AND THE ROLE OF INSURANCE

In my previous two posts (Part I, Part II), I've explored general awareness related to cyber security and ways to prevent breaches, two foundational elements of overall corporate health and risk management. As many of us know, however, it's impossible to fully

eliminate cyber risk, and the reality is that cyber incidents still occur. In this post, I will explore the types of breaches that are most likely, the ways to respond to these incidents, and the role CEOs can expect cyber insurance to play.

From an incident perspective, the two most common varieties of breaches involve either the theft of information or attempts to generate ransom payments.

Despite the important differences between these two types of breaches, step one in incident response is essentially the same: conduct initial forensics to identify the hole used by the bad actor and get it closed. From a talent perspective, day zero forensics is a highly specialized skill, and is one that, for most firms, is best outsourced to a private sector security firm.

If a breach poses a risk to an individual's rights and freedoms, you must notify the appropriate supervisory authority without undue delay; in the UK, this would be the ICO (Information Commissioner's Office), but across the world there are several national data protection authorities tasked with information privacy. If you are in the US and the breach includes the theft of highly meaningful data or the encryption of data / systems, it is also appropriate to immediately notify the FBI. (note: while the FBI provides meaningful support in areas like negotiating ransom payments, they are typically not equipped to conduct initial forensic analysis).

Once you have identified the source of the breach and have it contained, you can move on to dealing with the implications of the incident. At this juncture, the type of breach has a large impact on what needs to be done.

If the incident was primarily related to the loss of information, incident response should be focused on mitigating the downstream impact of this data loss. For corporate information, this likely includes an assessment of the competitive impacts of the lost data.

If customer / personal data was also taken (e.g. the well documented Target and Home Depot breaches in the U.S.), the task becomes much larger and should include a full-blown incident management team to handle internal and external communications, identity protection services, customer service, etc.

For ransomware incidents, the biggest short-term risk is often the ability to continue operating your business. The folks who conduct these attacks are looking for leverage, something that is maximized when a company is not able to conduct business until paying for a decryption key. For this reason, hackers will attempt to both encrypt / delete primary data stores as well as backups stored locally or in the cloud. If successful, they'll have done their homework and will establish a ransom payment request large enough to really hurt, but small enough to still get paid.

If you have cyber insurance – and at this point, every company should – your insurance provider will be closely involved with both the ransom negotiation and corresponding

recover support (e.g. selection of service providers to assist in decryption and downstream recovery).

It is important to note that the bad actors who conduct ransomware incidents do not specialize in customer support, and the decryption keys often only work in a partial manner. In many situations, we have seen firms recover only 40 – 60% of their encrypted IP.

Also, because encrypted systems are typically infected by breaches, firms will need to stand up new systems to run their business going forward, something that can be an onerous, long-term task. And very costly!

From a financial perspective, the good news is that firms can expect a good portion of the ransom to be paid by their cyber insurer. The bad news, however, is that when assessing the full cost of the incident, insurance will cover only 30 – 50% of the full financial impact of the incident. So, while it's vital to carry insurance, it's even more important to reduce the likelihood of a breach.

As with many situations, in the world of cybersecurity post Covid-19, an ounce of prevention is worth a pound of cure.

MEET THE AUTHOR

ANDREW DUNCAN

Partner

Andrew is a life-long consultant with a very successful and diverse background, having served in MD or CEO roles for several technology and services companies. Andrew has over 25 years of technology leadership experience at an executive level, with a strong client background in the consumer, financial and professional services sectors. He's lived and worked in Europe and North America and has built high-performing teams that have consistently achieved double-digit revenue growth. Andrew possesses a proven track record in the delivery of large-scale operations and technology transformation agendas across the B2C and B2B space. Andrew has also participated in numerous speaking roles over his career, most recently for Private Equity International, as well as the Business Forum at the Commonwealth Heads of Government Meeting.

Infosys® | CONSULTING

consulting@infosys.com

InfosysConsultingInsights.com

LinkedIn: /company/infosysconsulting/

Twitter: @infosysconsltng

Infosys Consulting is a global management consulting firm helping some of the world's most recognizable brands transform and innovate. Our consultants are industry experts that lead complex change agendas driven by disruptive technology. With offices in 20 countries and backed by the power of the global Infosys brand, our teams help the C-suite navigate today's digital landscape to win market share and create shareholder value for lasting competitive advantage. To see our ideas in action, or to join a new type of consulting firm, visit us at www.InfosysConsultingInsights.com.