DNV·GL

DNV GL - BUSINESS ASSURANCE

CREATING CYBER RESILIENCE

WHITE PAPER

SAFER, SMARTER, GREENER

RETHINKING INFORMATION SECURITY

There are so many alarming statistics on the topic of cyber security that it's difficult to isolate one data point that summarizes the issue in a business context. Simply put: businesses are under constant attack. It's a rolling chess match of moves and counter moves. Unfortunately, bad actors have an inherent advantage: this is all they do. They have one task. You on the other hand, have many.

Surveilling the threat landscape, we do find this statistic—from the 2019 Trend Micro Cyber Risk Index Survey(1)—to be particularly symbolic of where we are, and what we face: **80% of all businesses surveyed expect to be hacked this year.**

That is staggering. And perhaps worse, only 39% of the 400 executives and board members surveyed said their company has fully developed and implemented a cyber defense strategy.(2)

The expectation of being hacked shows the state of mind of organizations across the board, not just those who have been breached or who may fit a profile of "high risk" businesses (banks or hospitals, for example). Smaller and medium sized business are particularly vulnerable because of their relative lack of resources compared to Fortune 500 companies.

This tracks in parallel with the increasing sophistication, and nimbleness, of the threats. One of the rising hot spots is called formjacking, where fillable online payment screens are hijacked along with credit cards, home addresses, birth dates and other sensitive personal information. This underscores the vulnerability of transactional data, which is fundamental to online commerce and yet is significantly more exposed than corporate data contained behind firewalls.

But what's particularly noteworthy about the Trend Micro finding is the REASON so many businesses believe they'll be breached. It's not because of an exotic piece of technology they cannot afford, or some rainmaker cybersecurity professional they cannot recruit. Their biggest vulnerability is their own lack of alignment . . . employees and business processes ill-coordinated to prevent and / or recover from a breach.

> The reason so many businesses believe they'll be breached . . . is their own lack of alignment.

As reported in the study's findings: "A primary cause of these risks was found to be complex, misaligned organizations with a lack of security connectivity, scalability and agility, and too few qualified people to manage security systems."

All this lack insecurity doesn't seem to be for lack of effort, at least financially. According to Garnter Research, **spending on cyber security worldwide is approaching $124 billion per year.**(3)

Yet the threats continue to escalate. According to IBM, over the last three years, more than 11.7 billion records and over 11 terabytes of data were leaked or stolen in publicly disclosed incidents.(4) The costs are significant and steadily rising. Globally, the impact of a data breach on an organization averages $3.86 million, and in the US it rises to almost $8 million. High profile "mega breaches" can cost exponentially more; recently health insurer Anthem settled a federal suit for $115 million resulting from its 2015 breach that compromised 80 million health records.(5)

Breaches occur with such regularity that not being hacked is the exception to the rule. The battle has changed fundamentally from one of preventive defense to one of recovery-oriented offense. **The idea of cyber resilience shifts the emphasis of IT strategy from the perimeter, i.e., defending the network from outside penetration, to 360-degree readiness**, recognizing the hard cold fact that many – perhaps most – information breaches occur from within the organization.

People are coming to the realization that if they're targeting you, over a period of time, you're probably going to get hacked," says James Belt, cybersecurity expert at IntelliDyne, an IT consulting firm in Falls Church, Va. "But our biggest concern is internal breach, someone clicking on something in an email or doing something they shouldn't."

In this age of artificial this and cyber that, the single biggest risk factor is human error. According to one study, upwards of 90% of all successful corporate cyberattacks in 2017 could be attributed back to employee error.(6)

"Day to day most people take the path of least resistance," says Paige Needling, Information Security Sector Manager for DNV GL Business Assurance. "You're busy, you have things on your mind, and the simple or casual action is the one that leaves the door open. You don't get too many chances these days, the threats are pervasive and ongoing. One little slip and a breach can occur."

People leaving passwords on sticky notes attached to their computer monitors. Executives leaving laptops in their unlocked cars while they run into Starbucks . . . and using unsecured WIFI while sipping a latte. Throwing unshredded policy manuals into the dumpster. Revealing too much personal information on Facebook, like the names of children and pets (favorite passwords for many). All of these are points of entry for committed data thieves.

On top of that, external threats sometimes walk right through the front door of your office, lab or factory. Someone making a delivery, an unmonitored visitor . . . they swipe a thumb drive from a desk or leave one that is laden with malicious code.

This underscores the critical link between physical security and cyber security, something that is often overlooked in the headlines and 24/7 discussion of the Dark Web, bot networks and other high-tech threats. As companies fortify their technical defenses, attackers increase their use of social engineering and other exploits that combine physical and cyber techniques. Paper files are still widely used and frequently insecurely handled; they're still a ripe target for data thieves. On one recent example, a security consultant recently spent three minutes in a dumpster near a bank and came out with a trove of sensitive information, including: Wire transfers documents; copies of personal checks; personal financial statements; back account transaction history, and an entire intact laptop computer.(7)

> " . . . the simple or casual action is the one that leaves the door open."

IT SPECIALISTS ADOPT ISO 27001

IntelliDyne, LLC, is an IT consulting company helping clients address large scale data analytics and cyber security challenges. Because their customer base includes the federal government, IntelliDyne is under strict pressure to maintain highly secure information practices. Not just for cybersecurity, but also for its buildings and physical assets as well.

In fact, IntelliDyne sees security holistically, and works hard to integrate physical protection the defenses against online threats.

"You need to have a broader view of security for your organization," says Christina Coakley, Director of Security, and Facility Security Officer for IntelliDyne. "Creating a secure environment requires collaboration between the physical side and the cyber side. Without that connection, you are going to have gaps that can be exploited."

For IntelliDyne, IT expertise is not only part of running an effective business, it's what they do for a living. Working with government entities means the company is very familiar with prevailing information standards and compliance mandates. Programs such as NIST and FISMA are regularly part of the mix for federal clients.

When considering its own security profile, IntelliDyne chose ISO 27001 to bring it all together.

"We believed we were secure, but we wanted to see how good we really were," says Damon McWhorter, VP of IT Solutions and Services for IntelliDyne. "ISO forces you to examine your policies and procedures and to document them in a clear plan. I'm a very thorough person, and still I was surprised at the thoroughness of the certification audit. We found a number of things we were able to improve."

McWhorter likens ISO 27001 certification to earning a college degree: It provides an education but also generates a diploma that is universally recognized by others. "It's the difference between saying you're well prepared vs. being able to prove it," says McWhorter.

Going through the certification process was initially daunting for IntelliDyne, but rapidly became a comfortable, even energizing, activity.

"After you get used to the lingo, you realize it's a business process and actually gives your organization a lot of flexibility to determine how you're going to implement your security procedures," says McWhorter. "Unlike many other compliance programs, ISO isn't just a checklist; it's an overall structure that allows each business to decide how to implement security controls that meet the standard with the least disruption to existing business processes."

That kind of flexibility is crucial in confronting ever-evolving cyber threats. One minute it's DOS (denial of service), the next minute it's whaling or some other social engineering attack.

And in the final analysis, ISO 27001 goes beyond even security; it contributes to an overall ethic of excellence. "Getting certified was really about continuous improvement for our organization," says Coakley.

Coakley credits the standard's requirement for internal audits as an example of driving constantly forward. "You do a lot less guessing. By taking a hard look at results, we can adapt our security approach to what's actually happening. That makes us more effective."

What is cyber resilience?
Resilience has its roots in biology(8) and psychology —which is interesting as technology comes ever closer to mimicking living, biological behaviors—and reflects a system's ability to absorb disturbances and keep functioning. Resilience is deeply tied to systems thinking, which is one of the things that makes it so compatible with ISO standards.

Applied to information security, resilience is:

- The ability to bend but not break and to snap back into shape;
- The awareness and IQ to incorporate lessons learned and become even stronger in the process.

The underlying idea is to be so thoroughly prepared that it's almost as if disaster has already struck, and yet you are still operating at full business capacity. The single best thing you can do is to visualize a breach and "see" the pathways of response that you'll employ. This isn't about predicting it's about preparing.

Smart defenses can, however, alert you to malicious activity. Some of it will be highly targeted, like denial of service attacks, while other intrusions are quieter and more insidious. For example, as you read this there are probably dozens of phishing emails sitting in your company's inboxes. If you are using sensible IT techniques (VPN, port management, SSO, etc.), you are more likely to squelch the problem before it erupts, and the invaders will move on. Better yet, if you've trained and rehearsed your employees, they'll know to never click on an uninvited link or attachment.

The old paradigm of "secure computing" was based on the idea of zero breaches. The new, smart and resilient enterprise believes in elasticity. The difference is mindset, which directly determines allocation of resources. Protect your systems and information assets with every investment dollar you can muster. But don't expect to be perfect and don't be shocked when a breach happens.

Prepare for it. Anticipate it. Operate every day as if it's happened and you are accelerating through it.

Recovery is crucial, but true resilience demands rapid evolution, as well, so you can arrive at a more secure place. Resilience requires learning and adaptation. Otherwise, you are just restoring the same status quo that allowed the breach in the first place. Hardly desirable.

"Restoring operations after a breach is critical to resilience, but it's only the first step," says Paige Needling, Information Security Sector Lead for DNV GL Business Assurance. "You need a framework in place to create a new security profile that is even stronger than before the breach. Most organizations are not prepared for that second phase, which leaves them unnecessarily vulnerable to another disruption."

> Reslience is deeply tied to systems thinking, which is one of the things that makes it so compatible with ISO standards.

Everything about your security posture must be forward leaning.

It's a strategic challenge with implications for corporate leadership all the way up to the Board of Directors at larger companies. In fact, the World Economic Forum has created its Advancing Cyber Resilience project to promote responsibility for cyber security among boards.(9)

Connecting the Digital Dots: ISO 27001 Certification

The data doctors are clearly telling us the answer isn't a wonder drug; the solution is a healthier lifestyle. Skip the pharmacy and work on your own immune system. Start exercising and eating better. Make better choices about things within your control.

Applying this to a business context, the path forward is organizational vitality. Create clear understanding among staff about cyber risks and their roles in preventing breaches. Educate, train and rehearse. Repeatedly. Empower a CISO to create a resilient IT infrastructure and to be proactive in protecting company assets.

And get certified to ISO 27001. It is the one "technology" available to any organization that is specifically engineered to improve organizational alignment, which, after all, is THE core problem.

ISO 27001 is global standard designed to help organizations establish a holistic information security management system. The standard addresses the entire context of an organization, not just the IT function. Certification to ISO 27001 should not be viewed as an IT effort but rather as an enterprise commitment to total organizational security. This might seem like too large a scope, after all, hackers are not trying to crack into the cafeteria, or steal office supplies. Or are they? Never before has there been such a tight link between physical security and cyber security.

Some well-known cyber attacks started in less-known organizational departments, such as Target's 2013 breach originated by a HVAC supplier with access to Target's systems.(10) This particular example also highlights the need for organizations to have controls over suppliers with access to their systems—and consideration to enforcing ISO 27001 certification to its suppliers as well.

"As a security investment, ISO 27001 has far-reaching benefits," says Needling. "It goes well beyond technology, and helps you coordinate other critical business functions like finance, legal, communications and sales. It's the ultimate silo buster, but as a non-prescriptive standard allows each organization to determine its own best path as long as they fulfill the ISO requirements, one of which is to continually measure your progress and make adjustments to real-world conditions."

> ISO 27001 is the one "technology" available to any organization that is specifically engineered to improve organizational alignment.

To use a software analogy, ISO 27001 is not an application, it's an operating system. It forces an organization to have a clear, documented and executable game plan. Good intentions aren't good enough. Impressive budgets, while helpful, are not the answer. When the digits start to fly, what matters is organizational muscle memory. Transparency is critical.

You must communicate across departments, levels and functions. In a crisis, silos are your worst enemy. If IT detects an intrusion, that has to be shared with management, and then with the IR and PR departments. Things cascade outward from there.

The problem is that most organizations lack the internal protocols to communicate quickly and effectively between groups and across business functions. And when it comes to information security, the first instinct is usually to isolate the problem in the IT department. The urge to "quarantine" is healthy when it comes to the hack, virus or leak itself, but is a major drawback when dealing with the organizational and stakeholder impacts of a breach.

Spend more time on risk assessment . . . of third parties, vendors, supply chain etc. These are the players in your connected enterprise. They also form the basis of traceability, namely your ability to identify the source of a breach. Sometimes it might be obvious, such as direct assault via DOS or penetration attempt from a specific IP address. Other times, you may not know, and in some ways that is more troubling than the breach itself because you remain vulnerable. Every vulnerability thwarted is a not such a "loss" averted but a lesson learned. Having a plan not only sounds good – and reassures stakeholders – it makes your company twice as likely to quickly recover from a breach.

After a breach, 47% of companies with a fully-implemented plan were able to identify the cause of the breach and resolve it within one month, compared to just 26% of those without a complete strategy.(11)

ISO 27001 certification empowers exactly that kind of complete strategy. In certification parlance, it's known as a "non prescriptive" standard. That means organizations are not forced to follow a monolithic checklist. ISO 27001 sets forth a series of guidelines and "expectations" (requirements) but does not tell you how to run your operations. This flexibility is critical; it makes ISO 27001 as suitable to a Fortune 500 auto manufacturer as it does for a small parts company that supplies that large auto maker.

At the end of the day, each organization creates its own security. All the rules and guidelines in the world won't protect you if you are not vigilant and truly ready. Better yet, START with the idea that you've been hacked, and rehearse in detail what you're going to do about it. If you see your organization recovering quickly, with little or no damage to stakeholders, you're at the doorway of resilience. To step through, you need to get better than you were before.

References

1. Trend Micro CRI, https://markets.businessinsider.com/news/stocks/trend-micro-survey-finds-80-percent-of-u-s-businesses-expect-a-critical-breach-in-2019-1027944851
2. Lack of Strategy, A.T. Kearney, https://www.atkearney.com/web/global-business-policy-council/article?/a/2018-views-from-the-c-suite&utm_medium=pr&utm_source=prnewswire&utm_campaign=2018GlobalCSuite
3. Gartner Research, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
4. IBM Report (records lost) https://xforceintelligenceindex.mybluemix.net/
5. Anthem Settlement, https://www.databreachtoday.com/judge-approves-final-115-million-anthem-settlement-a-11399
6. Human Error; https://www.securitymagazine.com/articles/89664-human-error-we-meet-again
7. Dumpster Diving, CSO Online https://www.csoonline.com/article/2123810/identity-theft-prevention-a-real-dumpster-dive-bank-tosses-personal-data-checks-laptops.html
8. Definition of Resilience, https://www.ecologyandsociety.org/vol9/iss2/art5/
9. World Economic Forum, https://www.weforum.org/projects/partnering-for-cyber-resilience
10. Target breach; https://people.carleton.edu/~carrolla/story.html
11. Recovery, A.T. Kearney, https://www.atkearney.com/web/global-business-policy-council/article?/a/2018-views-from-the-c-suite&utm_medium=pr&utm_source=prnewswire&utm_campaign=2018GlobalCSuite

DNV GL BUSINESS ASSURANCE
1400 Ravello Road
Katy, TX 77449
Phone: (877) 368-3530
www.dnvgl.us/CyberResilience

DNV GL is one of the world's leading certification bodies. We help businesses manage risk and assure the performance of their organizations, products, people, facilities and supply chains through certification, verification, assessment and training services. We combine technical, digital and industry expertise to empower companies' decisions and actions. Partnering with our customers, we build sustainable business performance and create stakeholder trust across all types of industries. With origins stretching back to 1864 and operations in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.

© Copyright 2019 DNV GL Business Assurance