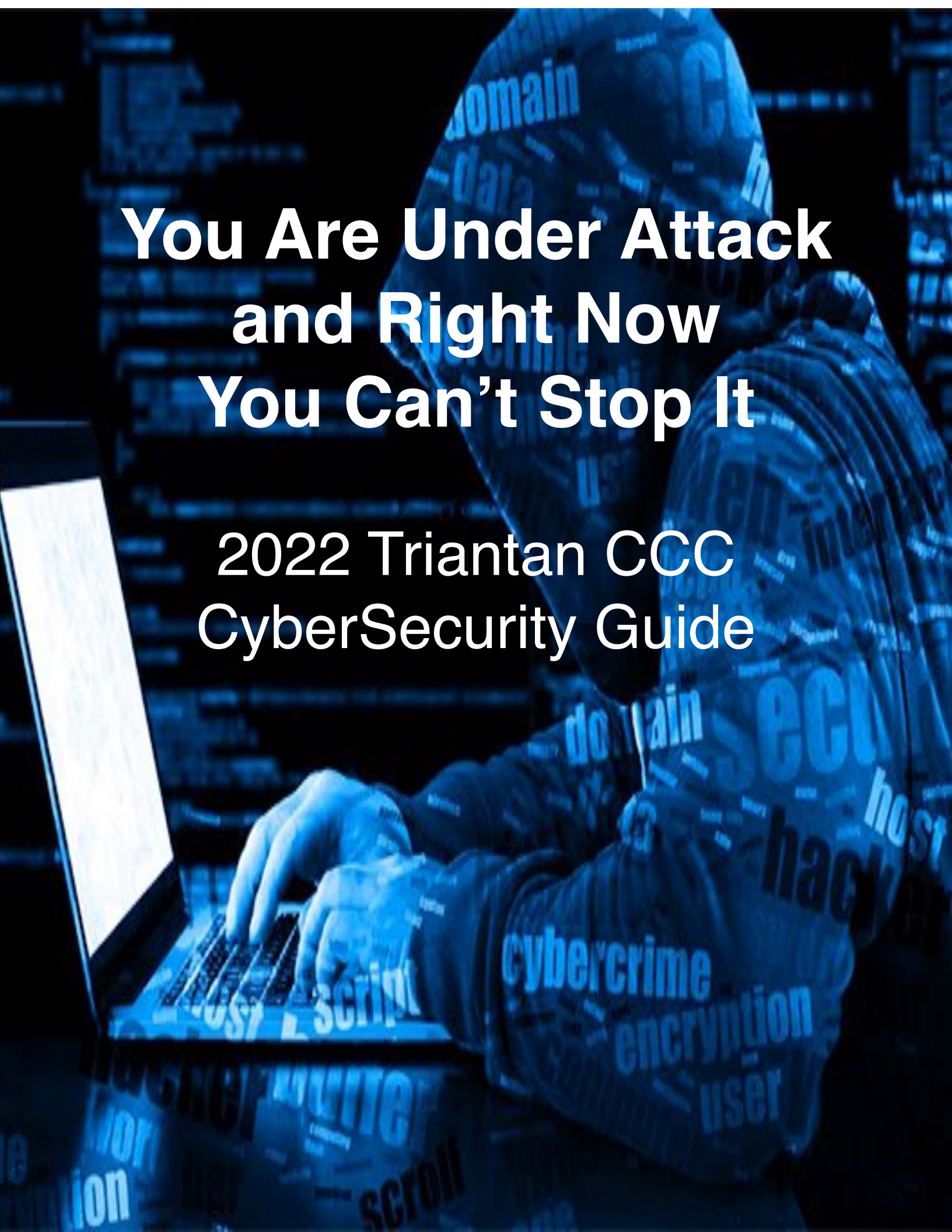


You Are Under Attack and Right Now You Can't Stop It

2022 Triantan CCC CyberSecurity Guide

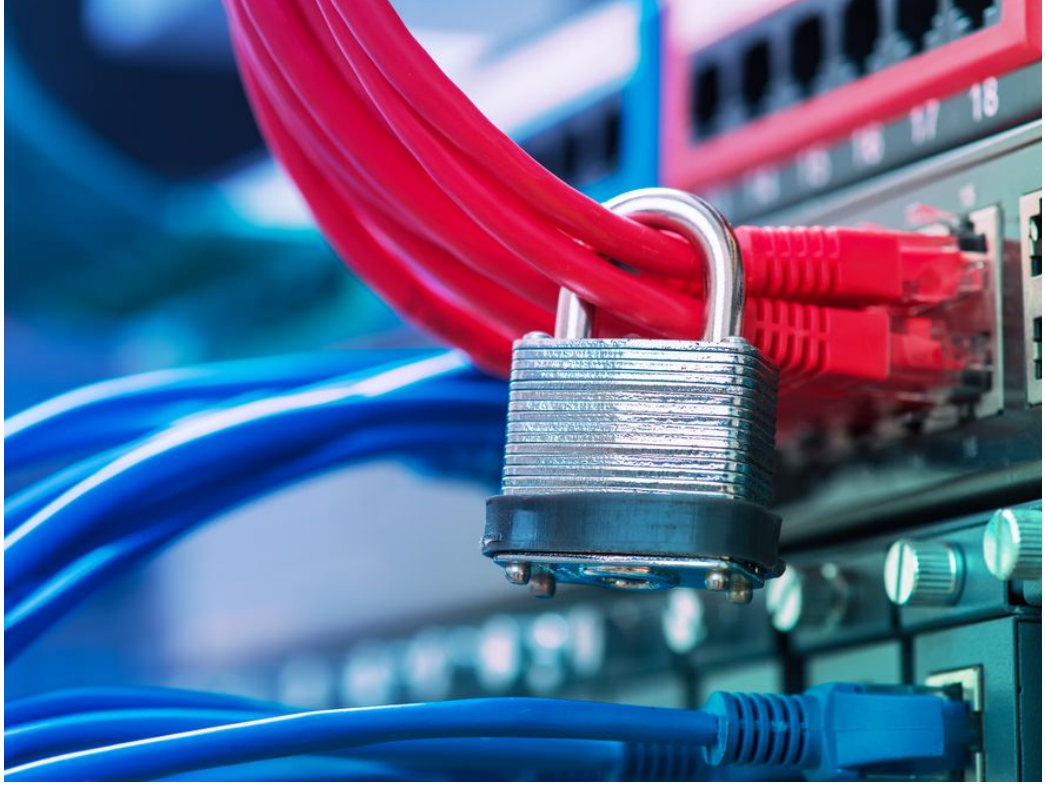


Table of Contents

"Even the bravest cyber defense will experience defeat when weaknesses are neglected."

— Stephane Nappo

Global Head Information Security
Société General

Concerned? You Should Be…

Cybersecurity and avoiding the threat of data breaches is going to be top-of-mind in 2022. Four trends seem to be already manifesting themselves:

1. Ransomware won't be going away anytime soon. There will be a continuation of attack vectors that have been plaguing businesses for years – ransomware being a key one. Major ransomware attacks will continue with cybercriminals utilizing increasingly inventive ways to pressure their victims. Expect increasing use of making threatening calls to company employees, and leaking or selling the organization's sensitive data online after an attack. In response to this, expect a renewed focus on preventing ransomware – and because over 90% of malware is delivered via email, expect organizations to ramp up their anti-phishing defenses in the coming year.

2. The need for cyber insurance continues to rise as do its premiums. Cyber insurance premiums, which now total about $5 billion annually, will increase on average 20% to 30% per year for the foreseeable future, according to Standard & Poor. The continued increase in ransomware attacks, the increase in data breaches, the increase in social engineering (phishing) and business email compromises, as well as the increase in governmental regulations and the financial consequences of non-compliance all team to drive premiums higher. Acquiring cyber liability insurance, despite high premiums, will help business offset some specialized costs that general liability insurance may not cover (compliance fees, data recovery costs, legal expenses).

3. There will be an increase in multi-vector attacks. Hackers are combining attack forms (not just phishing). The next logical step is to include social and communication platforms. Hybrid work has created huge demand for collaboration tools, and from a cybercriminal's perspective, they can be a treasure trove of company data that is often unsecured. Business needs to learn that it needs to be cautious with its use of email in terms of both accidental data loss and phishing attacks. It is a fact that employees tend to use corporate collaboration tools in a more casual and carefree way. How? Employee personal messaging styles easily bleed over into corporate collaboration. It's this feeling of ease and safety that hackers will look to exploit.

4. IT priorities will shift from training to technology. 2022 could be the year where cyber training programs finally hit their limit. Cyberattacks have already outpaced the defense that security awareness training (SAT) can deliver. Organizations are starting to realize that their investments in training aren't keeping them safe. Insiders continue to pose the biggest cybersecurity risk. Security teams are more aware than ever that training isn't enough to solve the problem, especially not on its own. More organizations will provide a technology-based safety net for employees as they carry out their work.

A cyberattack takes place approximately every 39 seconds or about 2,240 times a day according to the University of Maryland

85% of all data breaches involved small business victims

Only 24% of cybersecurity pros surveyed focus on prevention strategies

23% of data breaches were a result of human error

9-in-10 working adults report using their employer-issued devices for personal activities

52% of breaches were caused by malicious attacks with financial motivations

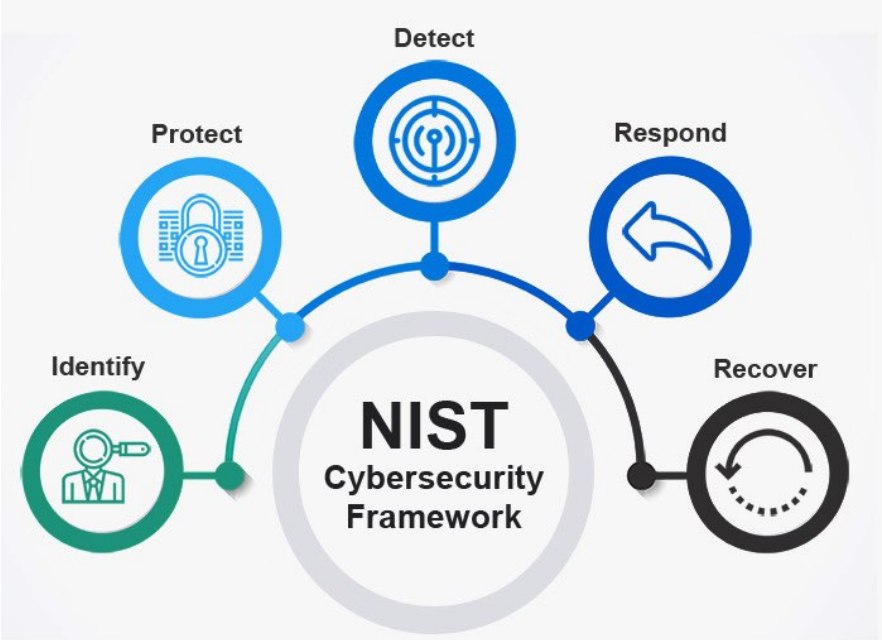
93.6% of malware has been observed to be polymorphic, meaning it has the ability to constantly change its code to evade detection

Only 34% of Businesses are confident in their ability to respond to a cyberattack or data breach

66% of organizations confirmed they either haven't reviewed or updated their data breach response plan since it was created or don't have a specific plan to review

Only 49% of businesses surveyed confirm they have Cyber Insurance coverage. Less than half could confirm their confidence of a total and prompt cyber incident insurance payout

Sources: Cybersecurity Ventures / 2020 Webroot Threat Report / IBM Cost of Data Breach Study 2020 / Kennet Research Study / Ponemon Institute Research / Great Horn / Risk Based Security Proofpoint Verizon 2020 Data Breach Investigations Report / Coveware Ransomware Report



It's Time To Get Familiar with NIST CSF

The NIST CSF is an organized group of cybersecurity controls designed to be applicable to businesses of all size. Issued by the National Institute of Standards and Technology, part of The Department of Commerce, it comprises those 5 core functions illustrated above, as well as 23 more categories of security controls. The NIST CSF is a ***voluntary*** framework for business, other than those that ***must*** comply due to law or regulation. Today, there is no enforcement of the NIST CSF, other than when it is implemented as part of another regulation, but this lack of enforcement is rapidly evolving as attacks multiply.

Given the reality of cyber breaches, today's corporate leaders and officers need to ask themselves ***What would happen if…***

- Your systems go offline without warning?

- All your company's private, critical data is stolen & encrypted by Ransomware Hackers?

Would you…

- Lose your biggest customers?

- Lose the trust of your clients, partners, and destroy your company's professional reputation?

- Be unable to do business for weeks, even months, as you deal with the fall-out?

- Know that you are meeting the agreed upon stipulations in your Cyber Insurance Contract?

If you are not taking appropriate steps and precautions, you could easily have:

No Cyber Insurance Coverage or Payout

No Revenue Production

No Protection from Lawsuits

No Recourse

So what's a seasoned professional to do…

Ensure Cyber Insurance Coverage is in place and that there will be Policy Payout in the eventuality of an attack

On January 5, 2021 a new law went into effect that offers 'safe harbor' – relief from fines and regulatory penalties after incidents, and early termination of audits, if an organization can demonstrate it has implemented a government-recognized cybersecurity program for at least 12 months.

Instead of thinking 'you can't afford to protect your data', you should be thinking 'you can't afford NOT to protect your data'

Even the Mightiest Do Not Provide Invincibility

Due to its global popularity, Microsoft 365 is the most targeted tech platform. In fact, 70% of all cyber-attacks target Microsoft Office products.

Many organizations that use SaaS apps like O365 operate under a misconception that it is the SaaS provider's responsibility to protect data and that organization SaaS backup isn't necessary. This is not the case. Microsoft and other software providers follow the "Shared Responsibility Model" where the SaaS provider is responsible for the software application uptime and its availability. Protection of business data ***is on the business***. This is clearly detailed in all SaaS agreements.

SaaS providers, like Microsoft, have best-in-class security and disaster recovery capabilities that protect against infrastructure threats, including hardware and software failure, power outages and natural disasters. However, they ***do not*** protect you from some of the leading causes of SaaS data loss. These include…

Human Error - Whether maliciously or not, employees can overwrite important files or delete business-critical information

Ransomware - The same tools that make SaaS apps optimal collaboration platforms also enable easy propagation of ransomware

Sync Errors - A third-party app sync error can ruin valuable SaaS data with absolutely no option to undo it

Insider Threats - SaaS vendors have no way to identify intent. If an authorized user makes a deletion request, it is viewed as legitimate. This makes employees and any compromised credentials effective cyberattack vectors

No Best Practices Implementation - The lack of dedicated "on-staff" cybersecurity professionals can lead to errors when trying to manage and implement SaaS apps and company policy

Office 365 Business Premium

"Microsoft Teams users warned that hackers are using it to spread malware"

- yahoo!finance 2.18.22

Protect your business from potential threats with a dedicated service for detection and response. Utilize 24/7 monitoring and alerting that detects and reduces the following vulnerabilities:

- Account break-ins
- Attacks by nation states
- Internal threats
- Phishing attempts
- Lateral O365 movement and events
- Data exfiltration
- Ransomware
- Business email compromise

"The evolving cyber threat and new stricter regulations will change the way businesses are impacted by cyber incidents: they will have to deal with business interruption, financial penalties, regulatory scrutiny and reputational damage in a way they haven't done before. All of these could be serious threats to a business's revenue, share price or even survival."

- Lloyd's

Get Compliant Stay Compliant

To reduce your liability, incorporating the following Best Practices will help…

Implement a data backup and disaster recovery solution

Secure your website

Use enterprise-level antivirus and anti-malware applications

Train employees about phishing and cybersecurity threats

Continually monitor your IT systems for issues

Patch your software

Create a password policy

Encrypt your data

Experts estimate that damage inflicted by cyber crimes will amount to $6 trillion globally in 2022. This is higher than the GDP of Japan. Currently, cyber attacks put 60% of SMBs (a client/server protocol that governs access to files and whole directories, as well as other network resources like printers, routers or interfaces open to the network) out of order. In response Federal and State privacy legislation is now driving cyber insurance mandates. Cyber insurance coverage and policy underwriting is no longer a few checked boxes with "yes or no" responses.

Cyber Liability Insurance (CLI) covers the financial loss that results from cyber events such as data breaches or ransomware attacks. However, just because an organization purchased and included CLI in its business insurance mix, does not guarantee that following a data breach all claims will be honored. It also does not guarantee how long the insurance company or insurance reinsurer's incident response and forensic teams will take to present final analysis and reports.

Just committing to a policy is not enough. You must also track and measure compliancy within the terms of the agreement. You must do this to insure that your contract is always valid, and will therefore payout in a timely manner in the event of an event. Non-compliance with the insurance policy requirements can lead to claim denial.

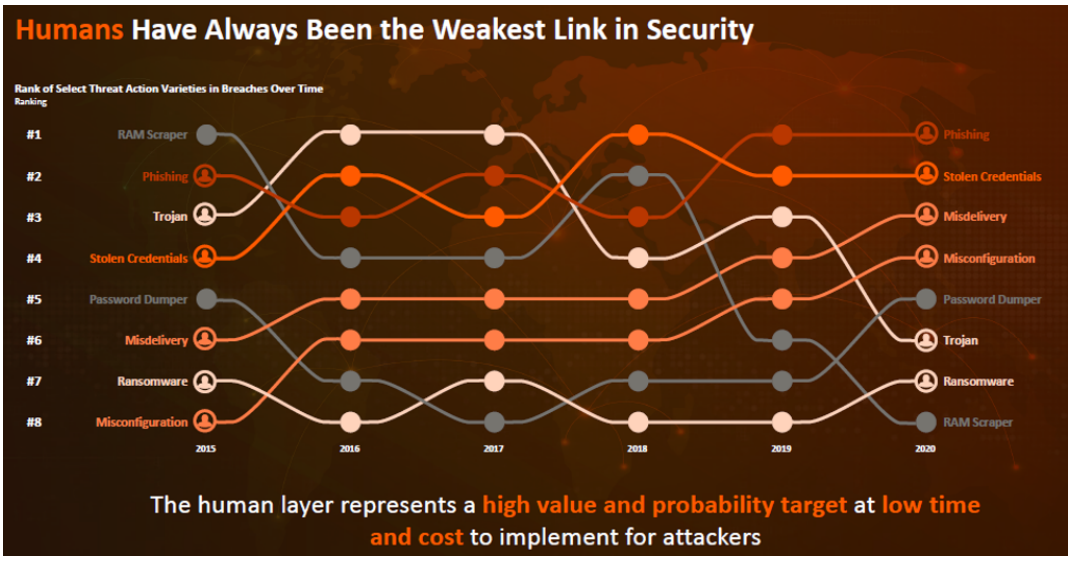
Nothing in business is ever "guaranteed". However, if CLI policy requirements are followed and there is investment in proactive security strategies and tools, a business can minimize the possibility of claim denials or delays. Make sure that your internal and external IT resources fully comprehend and support NIST and end-to-end data compliance standards.

Your Employees Know Better…

Think Again

85% of data breaches have a human aspect, according to a recently published Verizon Data Breach Investigations Report.

Organizations need to measure and understand the impact of employee risk on their overall risk posture and mitigate those risks proactively. Another study states that 60% of employees who failed a cybersecurity quiz actually feel safe from cyber threats, and incredibly, 74% of respondents who answered every single question incorrectly also felt protected. Comfort leads to carelessness which leads to open avenues for an attack.



How can this happen? Employees have a false sense of security and believe their organization's anti-virus has them covered. Unfortunately, with the firehose of spam and malicious emails that attack networks, 7-10% make it past in-place filters. This places your employees directly in harm's way.

An essential additional security layer is to have your employees be your last line of defense. Awareness Training on its own, typically once a year, is far from enough. Organizations also need to consistently and proactively test their systems. However, these simulated tests of groups of employees also don't work as a stand-alone effort. The good news is that together, conducted frequently and reinforcing each other, they can be combined to greatly increase effectiveness.

“It is no secret that cybercrime activity conducted in the dark web is rising exponentially, we believe that continuous threat intelligence and dark web monitoring are critical for organizations to identify and manage data breaches in a timely manner”

- Beenu Arora, CEO of Cyble

Beware the Dark Web?

The dark web is a part of the internet that's difficult to access without special software. It can be difficult to navigate once you gain access. Multiple layers of encryption allow people to browse and post information on the dark web with near anonymity, making it a go-to platform for buying and selling illicit goods and services.

Why Is the Dark Web So Popular With Criminals?

Its network makes it easier to hide your identity and allows people to anonymously create and host sites. Hence, criminals often use the dark web to buy and sell illicit goods and services.

Darknet marketplaces can be surprisingly similar to sites you find on the surface web—complete with limited-time sales, customer reviews and advertisements for organic products. However, criminals use these marketplaces to sell illegal products and services, including drugs, weapons and hacking software. Many identity thieves and hacking groups make money selling the information they steal on the dark web.

How to Protect Yourself From the Dark Web

The dark web isn't necessarily bad, illegal or dangerous. Lawful industries and governments use the dark web to gather and share information without revealing ID’s.

However, if you're the victim of identity theft or affected by a data breach, your information could be sold on the dark web. There are some steps you can take to help protect your company and stay ahead of identity thieves:

-***Be cautious when browsing the dark web.*** If you choose to browse the dark web, be mindful that you don't know where a .onion address will take you. You could unwittingly wind up on a site that tries to install malware on your device.

- ***Use unique passwords for your accounts***. If your account information is stolen, it's only dangerous if an identity thief can actually use it. Creating unique passwords for all your online accounts can help limit the impact of a single data breach. If you suspect your account information may have been compromised, change your passwords immediately.

- ***Update your passwords.*** Regularly changing your passwords even in the absence of a threat can also make your account information less useful. A password manager can help you create and store strong passwords, and may even perform regular security checkups for you.

- ***Sign up for dark web monitoring.*** A dark web monitoring service will look for your information on the dark web and inform you if it finds anything. The forewarning will let you know which information is compromised, and gives you a chance to take steps to secure your data and accounts.

- ***Lock or freeze your credit reports.*** Locking or freezing your credit reports can keep someone from opening an account in your name, even if they have your information.

There are other ways to protect your information online as well, such as being mindful of what is shared on social media, closing unused accounts and avoiding phishing attacks. This points to educating your employees and installing programs to protect against open attacks.

You cannot manage what you cannot see!

In addition to Security, Compliancy, Risk Mitigation, and HR Best Practices, company leaders are required to consider and maintain (or exceed) acceptable business productivity objectives and ever expanding bottom line numbers. To assist executives and managers in meeting these productivity measures, organizations should include a superior reporting package on internal organizational Internet/Web Site Usage and Utilization. This package provides a comprehensive yet easy way to utilize standard or customizable reports that supply specific Web Use information. Your managers obtain reliable metrics, easy-to-read dashboards and analytics, and management-ready audit reports.

Top User by Time

	UserName	Visits	Time Online	Time Online
1)	Alexis Humphrey (ahumphrey)	3,079	45:25:35	7%
2)	Uriel Hartman (uhartman)	2,547	33:01:28	5%
3)	Rayan Waters (rwaters)	13,254	32:36:03	5%
4)	Aaden Manning (amanning)	1,399	30:00:26	4%
5)	Gregory Farley (gfarley)	1,349	25:28:27	4%
6)	Marc Quinn (mquinn)	1,883	22:47:15	3%
7)	Deanna Hawkins (dhawkins)	3,569	20:34:58	3%
8)	Eugene Sampson (esampson)	9,029	18:47:57	3%
9)	Keegan Nash (knash)	7,388	18:31:32	3%
10)	Athena Love (alove)	1,412	16:48:19	2%
11)	Audrey Fitzgerald (afitzgerald)	10,295	16:17:04	2%
12)	Halle Richards (hrichards)	5,725	15:10:01	2%
13)	Ella Malone (emalone)	640	10:54:18	2%
14)	Paulina Buchanan (pbuchanan)	4,763	10:09:43	1%
15)	Marlene Cline (mcline)	1,797	10:03:27	1%
16)	Gabrielle Robertson (grobertson)	925	9:05:52	1%
17)	Gianna Mosley (gmosley)	3,251	8:28:56	1%
18)	Ricardo Watts (rwatts)	1,803	8:18:50	1%
19)	Donte Wilcox (dwilcox)	3,581	7:27:28	1%
20)	Alondra Gaines (againes)	2,323	7:24:19	1%
21)	Asia Bradshaw (abradshaw)	6,024	7:16:16	1%
22)	Carrie Beasley (cbeasley)	364	7:08:59	1%
23)	Annabella George (ageorge)	1,787	6:51:53	<1%
24)	Tia Cobb (tcobb)	1,618	6:22:12	<1%
25)	Shaun Compton (scompton)	5,623	5:29:19	<1%

<< < 1 > >> 25

As mentioned previously in this paper, a passing grade for most compliance insurance policies requires verification of the implementation and ongoing utilization of company-mandated best practice monitoring and alerting tools. These types of monitoring packages assist in this verification.

What exactly do these reporting packages provide?

- Easily see how much time users are spending online
- Accurately identify actual user clicks, providing detailed and clear useful data
- See time online by friendly Website name, not ambiguous Domain Name
- See only real web browsing activity
- How often users are connecting via VPN