ISSUE 92 | FALL 2022

BIZGROWTH STRATEGIES

IDEAS TO COMBAT CYBERSECURITY THREATS

CYBERSECURITY SPECIAL EDITION

Threats from the Dark — Is Your Business at Risk?

Cybersecurity: What Every Business Needs to Know

Open Enrollment Cybersecurity Checklist — Is Your Data Secure?

Closing the Resource Gap in Cyber Safety: Cybersecurity Meets the CISO

Plan Sponsor Cybersecurity Best Practices

Tips to Prevent Payroll Fraud

CBIZ Your Team.

In This Issue

CBIZ

CBZ

CBIZServices

To subscribe to this newsletter or a variety of others, visit cbiz.com/newsletter-subscribe.

You can also call us at **1-800-ASK-CBIZ** (1-800-275-2249).

Cyberattacks are becoming more frequent and sophisticated, making a recovery from them increasingly difficult. Without preparation, a cyberattack can be devastating to your business, having severe operational, financial, legal and reputational implications.

A "set it and forget it" cyber risk management approach is simply not an option. Further, the prevalence of cyber breaches means cybersecurity is no longer solely an IT concern. Elevating your information security from functional to effective takes a robust set of elements, processes and people working together toward a common goal.

Our professionals have developed these articles and resources to help you protect your organization from these attacks in multiple operational areas.

Threats from the Dark — Is Your Business at Risk?

What Is the Dark Web?

The internet is comprised of three layers:

Surface Web

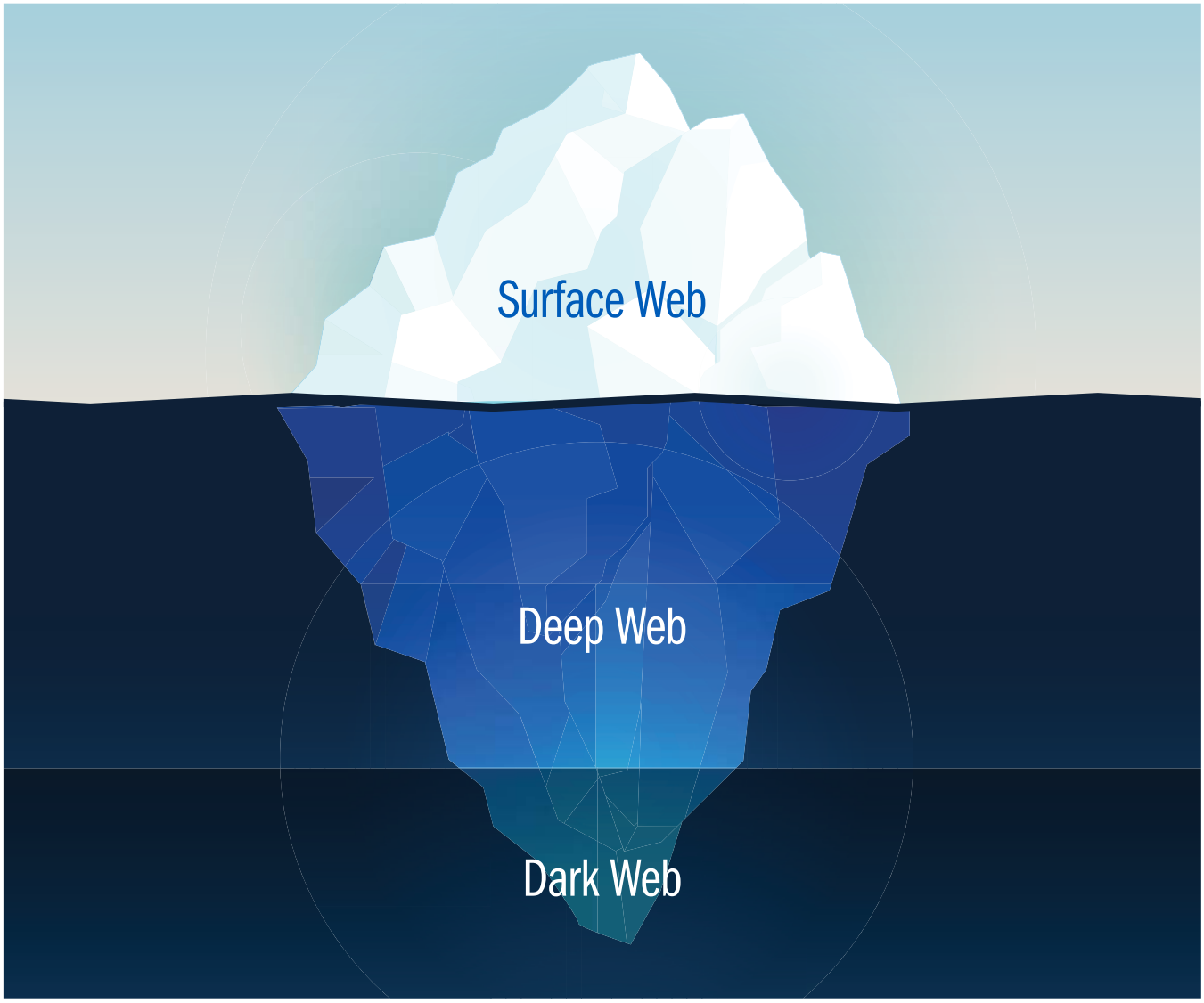
- What many refer to as the world wide web
- Small portion of accessible digital content

Deep Web

- Typically password-protected
- Data is only accessible through a database query

Dark Web

- High levels of illegal activity
- Hidden marketplace
- Private computer networks communicate & conduct business without divulging identifying information
- Uses encryption software so visitors/owners remain anonymous & can hide locations



Security Measures to Consider

As a business leader, consider these questions to help assess how your operations and supply chain vulnerabilities might be affected:

- Does your risk management group or IT security team monitor darknets for activity related to your organization?
- Have you had a breach and, if so, do you know if company data has been published on darknets?
- Do you know if your employees reuse passwords that have been published in other companies' data breaches?

Policing the Dark Web

Using a dark web monitoring service can help businesses stay ahead of cyber threats. An experienced risk advisory team can monitor threat intelligence for your business. When selecting an advisor, be sure they will:

- Investigate threat actors
- Search for bitcoin wallets and addresses
- Assess darknet brand exposure
- Identify threats on darknet forums
- Monitor for leaked credentials
- See inside authenticated chat rooms
- Track vendors on marketplaces
- Access historical darknet records

Connect with a CBIZ Cybersecurity specialist today.

Cybersecurity

What Every Business Needs to Know

Cyberattacks have surged in frequency and sophistication. They can range from phishing to viruses to ransomware. Once hackers have gained access to your organization's systems they can steal confidential information or financial assets, corrupt data, and cause operational disruption or shutdown.

Are you protected from potential network and privacy exposures? Any business that uses technology needs to know the facts and risks associated with data breach liability and not having proper network security, privacy and cyber protection.

The high cost of data breach

$9.44M

Average cost of a data breach paid by U.S. companies

55%

of breaches are caused by malicious attacks. System glitches (24%) and human error (21%) are the next top causes.

52%

of data breach costs come in the first year; approx. 29% comes in the next 12-24 months; the final 19% comes more than 2 years later.

$4.35M

is the average cost of a **malicious breach.**

82%

is the difference in breach cost when **security AI** was deployed vs. not deployed.

Nearly **40%**

of the average total cost of a data brach **stems from detection and escalation.**

80%

of organizations have experienced **more than one breach.**

Data breach by the numbers

1.4B records exposed Jan. 1 - June 30, 2022

277 days average time to identify and contain a data breach

HEALTH CARE	FINANCIAL	PHARMA
$10.1B	$5.7B	$5B

TECHNOLOGY	ENERGY	INDUSTRIAL
$5B	$4.7B	$4.5B

4 Reasons you need cyber liability/security protection

1. Stringent laws/ regulations
2. Advances in technology
3. Global outsourcing
4. User error

Connect with a member of our team for a no-obligation consultation and risk assessment.

Source: 2022 Cost of a Data Breach Study sponsored by IBM Security with research independently conducted by Ponemon Institute LLC

Closing the Resource Gap in Cyber Safety: Cybersecurity Meets the CISO

When the pandemic shut down our lives, our virtual worlds booted up. The ways we work, learn, shop and socialize are forever changed, and, in some cases, people don't want to go back — literally. But tradeoffs abound; moving life online put IT executives and their teams into overdrive at a time when IT employees are hard to find and keep. Add in the fact that, according to a study by McAfee Enterprise and FireEye, four out of five companies report an uptick in cyberthreats since the coronavirus hit, and we've reached a boiling-point need for cybersecurity solutions. CFOs know their sore spots; technology concerns find a place on many, if not most, surveys that take the pulse of what financial leaders worry about most.

The Cost of Cybercrime

It's a fear grounded in common sense — and cents. According to Cybercrime Magazine, at the end of 2021, experts predicted the total loss from cybercrime that year would top $6 trillion, with a 15% increase expected per year between now and 2025. Seventy-nine percent of global businesses experienced downtime due to a cyber threat during a peak season. These threats and their costs are intensified by global events, including Russia's attack on Ukraine.

Cyberattacks are not limited to high-profile and public companies, and no industry is immune. According to Yahoo Finance, in general, cyber safety solutions are facing a period of "remarkable growth" owed to factors including surging cyber threats and increased governmental data privacy regulations.

The Talent Crunch Meets IT

Inflation and the talent crunch make for the perfect storm when it comes to addressing cybersecurity. Because of this, companies may lack funding and resources to tackle these issues as thoroughly as they would like. That gap makes for existing structures and policies that can miss rapidly developing changes in the world of cybercrime.

Many experts turn to common tools for cybersecurity — conducting risk assessments, educating employees, developing response plans and policies, and securing data. Companies may also then consider securing or renewing cybersecurity insurance. These are sound practices that every business should have as a baseline in addition to thinking about and addressing the specific cybersecurity challenges your business faces, including calling in a second set of eyes.

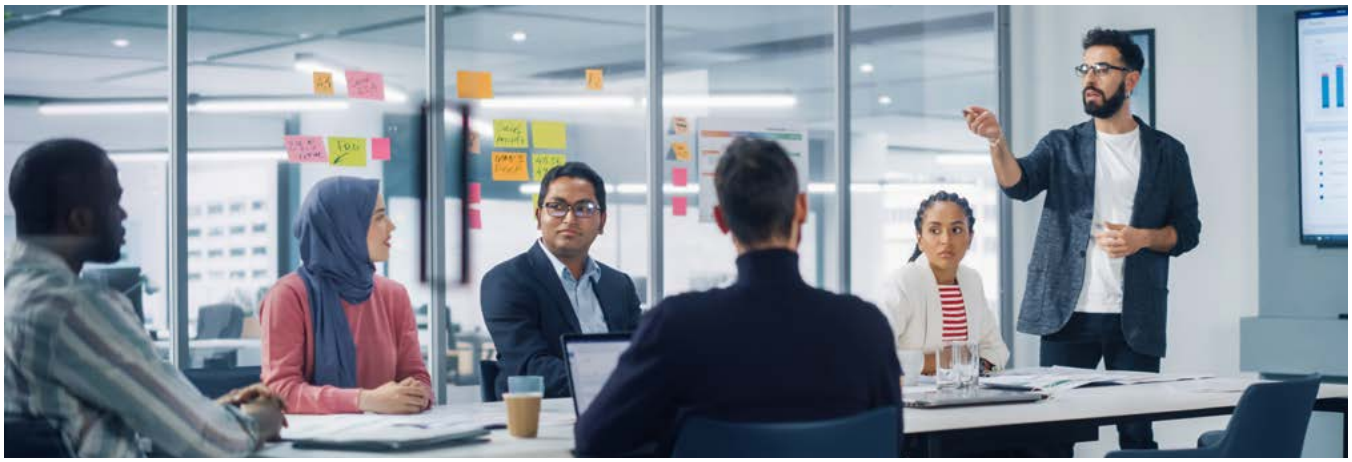
Cybersecurity & the CISO

A new kid on the cybersecurity block is the Chief Information Security Officer (CISO). Having a CISO at the table has become more possible now that the table is often virtual. A CISO can be an internal position or an external, fractional partner who supports existing leaders and teams. That means top-notch talent can give a second look at a company's technology needs and help advocate those needs to leadership. CISOs aren't just cyber experts; they're also experienced relationship builders. With a seat on the C-suite, a good CISO can, for example, help liaise between IT and leadership to rationalize and secure the resources needed to protect a company from cyber threats.

The advantage of CISOs is their ability to partner with existing IT executives and teams while also providing an objective, external perspective, just as a financial auditor supports the work of internal accounting teams and CFOs. For those who work day in and day out with existing systems, it can be hard to see blind spots. Having an external advocate can help bolster internal recommendations or troubleshoot problem areas.

The shift to remote work comes with opportunities and challenges. The CISO represents a unique chance to meet increased cyber threats and cybercrime ushered in by the ways we now live, work and play online — and, at least for now, that change is here to stay.

Connect with a CBIZ Financial Services expert today.



Plan Sponsor Cybersecurity Best Practices

The Department of Labor (DOL) issued three guidelines related to cybersecurity — tips a plan sponsor should look for in a provider, processes plan providers should have in place and online security tips for participants and beneficiaries.

According to the DOL, plan providers should have best practices and processes in place to protect plan assets, including but not limited to the following:

- Have a formal, well-documented cybersecurity program
- Conduct annual risk assessments
- Use third parties to audit the program
- Have strong access controls
- Conduct periodic cybersecurity training
- Encrypt sensitive data
- Have strong technical controls that meet security best practices
- Appropriately respond to any cybersecurity breaches

Plan fiduciaries also have responsibilities in this regard. The DOL requires plan fiduciaries to prudently select and monitor their providers, the intent of which is to safeguard plan assets. As a cybersecurity breach could affect participant accounts, plan fiduciaries should consider the following:

- Ask the provider about their cybersecurity practices, procedures, policies and audit results, and compare them to what others in the industry are doing
- Ask the provider how they evaluate their procedures and what level of security standards they meet
- Evaluate the provider's cybersecurity track record based on public records
- Ask the provider about any prior breaches, what happened and what was done to resolve the issue
- Ask the provider about any insurance coverage they have that would cover any losses due to cybersecurity breaches
- Ensure any contract with a provider requires ongoing compliance with security standards
- Beware of any language in a service contract that limits the provider's responsibility for any IT security breaches

The DOL believes plan participants and their beneficiaries also have a responsibility to help keep their accounts secure. The DOL suggests participants/beneficiaries:

- Register their account and monitor it regularly
- Use strong and unique passwords
- Use multi-factor authentication (MFA)
- Keep contact information current
- Close/delete any unused accounts
- Consider not using 'free' Wi-Fi
- Don't share passwords, accounts or other sensitive information with an unknown person, even those posing as a known person; it could be a phishing attack trying to obtain this information to gain access to accounts
- Use anti-virus software and keep it and all apps current
- Know how to report identity theft and cybersecurity attacks

Connect with a CBIZ Retirement & Investment Solutions specialist to learn more.

Investment advisory services provided through CBIZ Investment Advisory Services, LLC, a registered investment adviser and a wholly owned subsidiary of CBIZ, Inc.

Open Enrollment Cybersecurity Checklist — Is Your Data Secure?

The sheer amount of data being passed from employers to benefits brokers to insurance carriers during open enrollment puts organizations at serious risk for cyberattacks. From employee social security numbers to confidential health histories to beneficiary details and more, it's essential that you take action to protect this massive volume of valuable information.

What are the necessary precautions to safeguard your open enrollment data, and how can you be sure you're prepared to combat any cybersecurity threats that may arise? This interactive checklist can help you find out.

INSTRUCTIONS: Answer the questions below. Each response will be given a numerical value depending on the answer. After completing the questions, decode your score using the scale at the bottom of the page.

SCORING: YES = 0 points | NO = 2 points | UNSURE = 2 points

Questions	Yes	No	Unsure	Score
Have you shifted from paper enrollment forms to an online open enrollment platform to ensure increased security?				
If so, does your online enrollment software require passwords and multi-factor authentication before access to valuable data is granted?				
Are employees required to review their home address, email address and other personal information each enrollment period to ensure accuracy?				
Have you considered forgoing the use of employee social security numbers for enrollment and instead assigning employees individual identification numbers?				
Do you know exactly where your organization's sensitive data is housed — whether it's with a vendor, your broker or elsewhere?				
Have you worked with your IT department to ensure your organization's anti-virus software is up to date?				
Have you trained employees on how to identify sophisticated scams, such as phishing or smishing messages that are delivered via email or text message?				
Have you tested employees' knowledge of phishing and smishing attempts by sending test messages?				
Have you discussed cybersecurity with your enrollment vendors and asked the necessary questions to ensure maximum protection?				
Do you have a plan that is ready to be implemented in the event of a cyberattack, including appropriate contacts, IT procedures, post-breach employee materials and more?				
		Total Score:		0

Decoding Your Score

If you scored 0-6: It's clear you've put careful thought and consideration into cybersecurity ahead of open enrollment. You've taken the necessary precautions to mitigate the risk of a cyberattack while also preparing an action plan should an attack occur. Keep it up!

If you scored 7-14: You've started the process of preparing for a potential cyberattack, but there's more you could do to protect your employees' data prior to and during open enrollment. We recommend setting up a consultation with a benefits expert to talk about additional safeguards you can put in place to further reduce the chances of a data breach.

If you scored 15-20: While you've scratched the surface of cybersecurity prep, there's much more to be done to ensure your employees' enrollment data is adequately protected. Before you begin the open enrollment process, talk to an employee benefits professional about implementing a cybersecurity training program, asking your vendors the right questions, setting up secure online enrollment software and more.

Connect with a CBIZ Employee Benefits expert today.

Tips to Prevent Payroll Fraud

You can never be too careful when taking steps to protect your employees' payroll funds. There are many scams that others use to attempt to reroute payroll funds to themselves, one of which is a prepaid debit card ploy.

When hackers use this tactic they send an email to a payroll professional from what appears to be the employee's actual email address, usually personal email, requesting that the direct deposit is changed to deposit funds onto a prepaid card. For the tactic to work, the payroll professional must change the direct deposit information in the system without verifying the change with the employee, which can result in losses to the employee or the organization.

Stay Ahead of the Hacker

- Verbally confirm all direct deposit changes with the employee requesting the change.
- Speak to employees face to face or by phone.
- When calling an employee, use a phone number you have on file, not a phone number listed in the email you received requesting the change.

Other Considerations

Using a prepaid card to receive a direct deposit is not a definite indication of fraud, as some individuals legitimately use them. However, direct deposit fraud often involves a prepaid card because it's difficult to track the fraudulent activity. Once funds are deposited, fraudsters are waiting in the wings to drain the accounts quickly, which means the likelihood of recovery of any funds sent to fraudulent cards is very low. Also, prepaid card companies typically do not have a phone number to reach a live representative, so any attempt at recovering funds is through email, and response time is usually slow.

Connect with a CBIZ Human Capital Management professional for more payroll tips.