Data Privacy and Cybersecurity: Not Just a Big Company Problem

Session Sponsor

ESC
Essential StaffCARE

2021 ASA
STAFFING LAW
VIRTUAL CONFERENCE

Data Privacy and Cybersecurity: Not Just a Big Company Problem

Threase A. Baker, TSC, CSP, *president*, ABBTECH Professional Resources

Maureen Dry-Wasson, Esq., *vice president, group general counsel, and global privacy officer*, Allegis Group

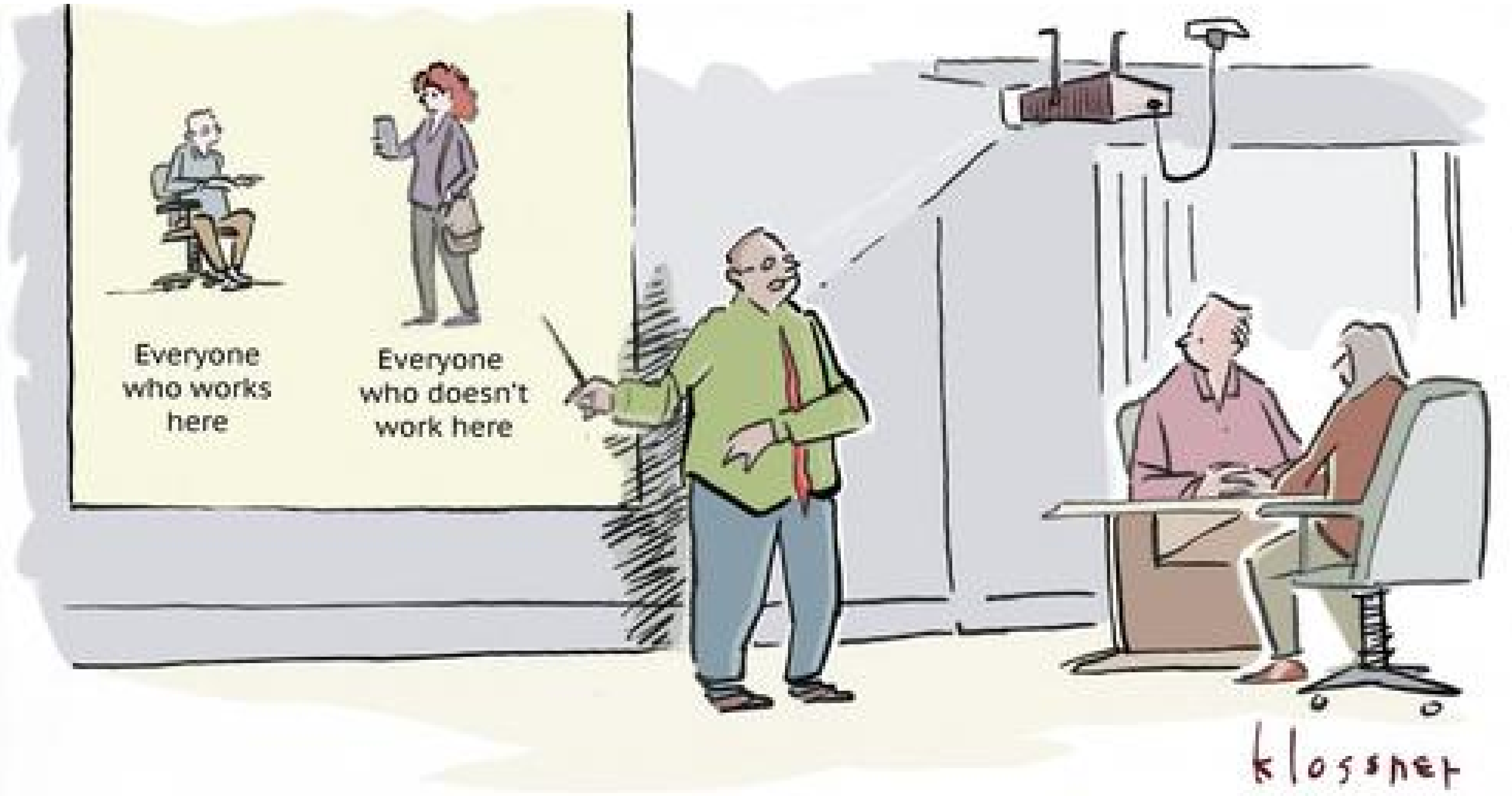
Michael Jones, Esq., *chief privacy officer*, Randstad USA

Bob Thompson, *president*, World Wide Specialty Programs Inc.

2021 ASA
STAFFING
LAW
VIRTUAL
CONFERENCE

Today’s Discussion

1. Statistics
2. Types of breaches
3. Why insurance
4. How to prevent
5. Additional resources and takeaways



" WE'VE NARROWED OUR SECURITY
RISKS DOWN to THESE TWO GROUPS."

Do You Know?

1. **Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. Cybercrime is projected to cause damage of over $6 trillion annually by 2021, up from $3 trillion in 2015. (Cybersecurity Ventures)**

2. A typical data breach remains unnoticed by the concerned organizations for up to six months, and even the major IT players are on the of such organizations. (ZD Net)

3. Small businesses are severely affected by data breaches and cyberattacks; 43% to be precise. Only 14% of small businesses rate their ability to mitigate cyber risks, attacks, and vulnerabilities as highly effective. Cyberattacks are the primary reason many small companies go out of business. (Small Business Trends)

4. The most targeted platform for hackers is Windows. Android comes next. (Computer World)

5. Information loss is the most expensive component of a cyberattack, with 43% of costs involved in it. (Accenture)

6. The Equifax breach has cost the company over $4 billion in total so far. That's how much stock market value Equifax lost in the week after the credit bureau revealed that it was hacked, compromising the personal information of about 143 million people. (Time Money)

Do You Know—Continued

7. **Considered as one of the fastest-growing malware threats, more than 4,000 ransomware attacks have occurred every day since 2016. Ransomware targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive information, disruption to regular operations, and potential harm to an organization's reputation. (FBI)**

8. Around 94% of targeted emails use malicious file attachments as the payload or infection source. 91% of cyberattacks begin with a "spear phishing" email, which is an increasingly common form of phishing that makes use of information about a target to make attacks more specific and personal. (KnowBe4)

9. **Ransomware costs include damage and destruction of data, downtime, lost productivity, forensic investigation, and reputational harm. Businesses may have been attacked by ransomware every 14 seconds by the end of 2020, up from every 40 seconds in 2016. (FBI)**

10. **Phishing attacks have affected around 76% of businesses in the last year. (Wombat Security)**

11. Spam emails that mention the hottest topics in the world news agenda are a constant feature of phishing. This trend is unlikely to change any time soon. (Kaspersky)

12. About 30% of phishing emails are opened by users, and 12% of those users click on the infected link or attachment. (Verizon)

Cyber or Privacy Breach Risks

“There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category; those that have been hacked and will be again.”
Former FBI Director Robert Mueller (2012)

- **Six areas of concern:**
  - Social engineering
  - Hacktivists
  - Employees
  - Vendors
  - Ransomware
  - Denial of service

Our Disaster Recovery Plan Goes Something Like This...
HELP! HELP!
DILBERT
By Scott Adams

How to Prepare

- **Make an incident response plan**
  - A *single* plan
- **Identify key vendors**
- **Practice, practice, practice**

How to Practice

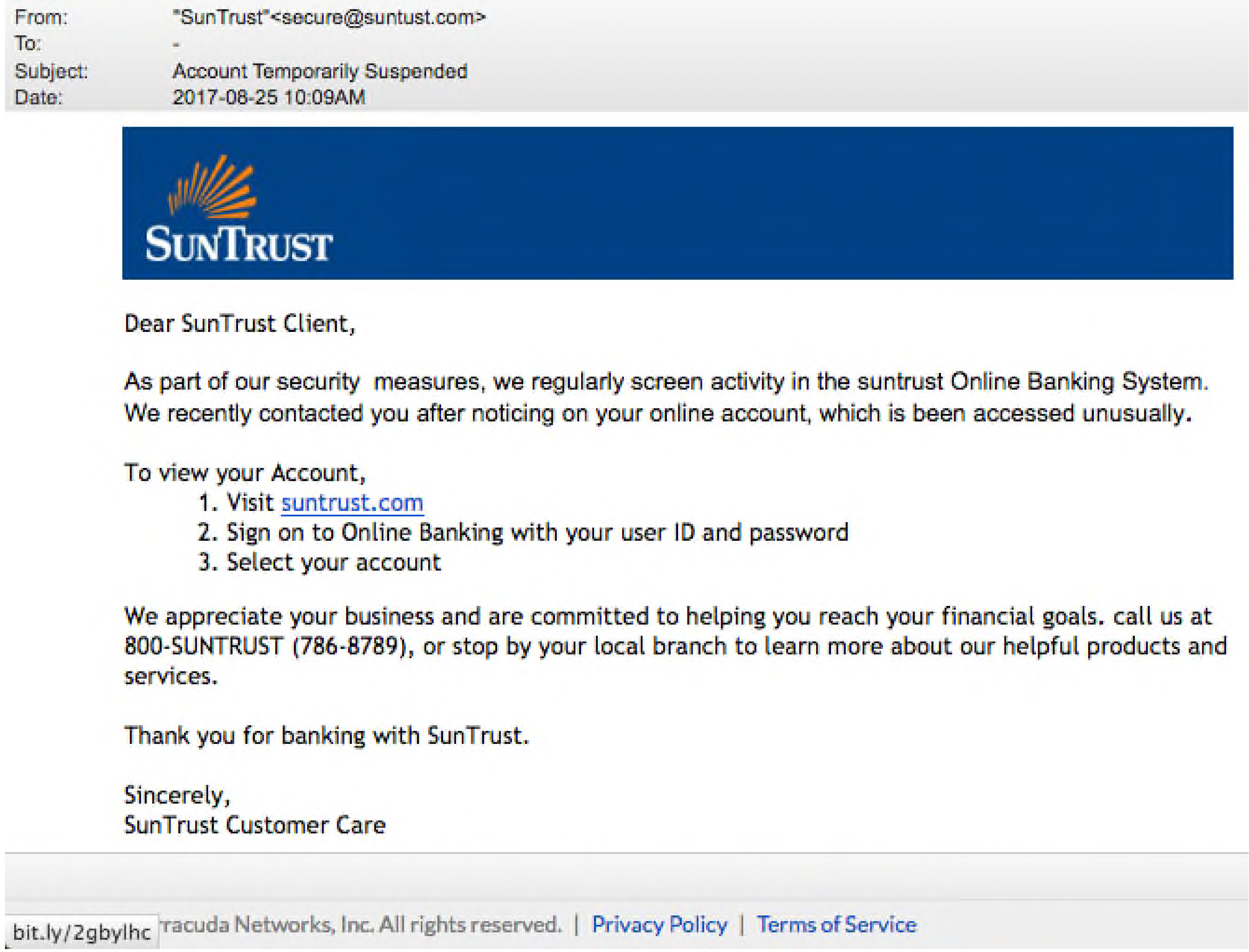
- **Communicate how to report incident to all employees**
- **Annual training for all employees**
- **Phishing tests**
  - Phishing is a leading root cause
- **Tabletop exercise for response team**
  - Every 12–18 months

Phishing Example: Account Suspended

You might receive a notice from your bank—or another bank that you don’t even do business with—stating that your account has been suspended. According to the email, your bank has discovered unusual activity and has decided to shut your account down to protect you.

The email will then ask you to click on a link to reactivate your account—leading you to a fake page that asks for your user ID and password.

How can you tell it’s fake?
There are usually several clues that such emails are fake. First, look for spelling or grammatical errors. In the example above, supposedly sent by SunTrust, you’ll see that the sentence “We recently contacted you after noticing on your online account, which is been accessed unusually” doesn’t really make any sense.



From:	"SunTrust"<secure@suntust.com>
To:	-
Subject:	Account Temporarily Suspended
Date:	2017-08-25 10:09AM

SunTrust

Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,
1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

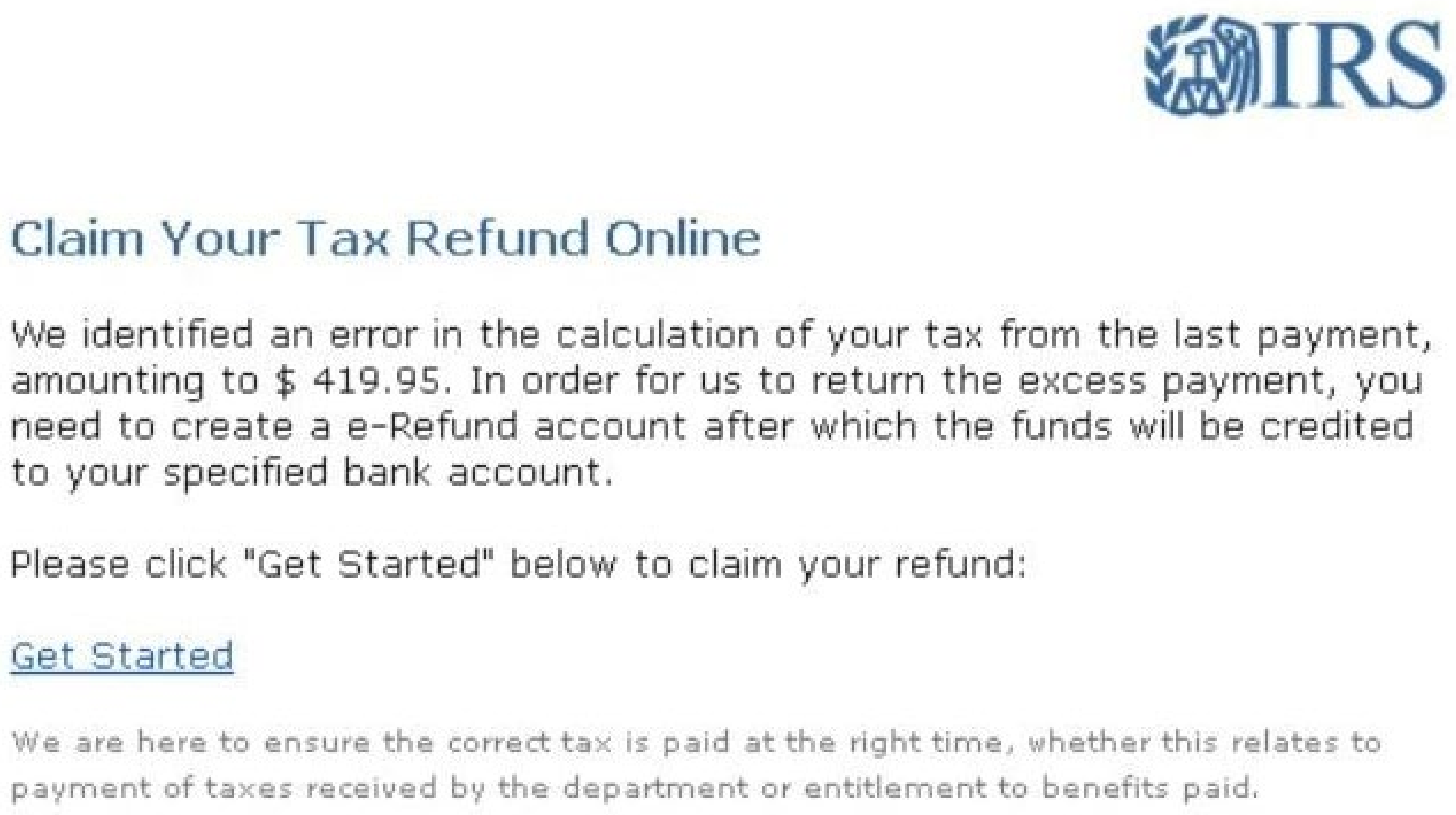
bit.ly/2gbylhc racuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

Phishing Example: Tax Refund Scam

Getting an unexpected windfall of cash? If someone sends you an email saying that you’re due a refund or cash prize of some sort, it’s usually a scam. Consider the IRS refund phishing attempt.

The email that looks like it comes from the IRS. The headline will promise that you are owed a refund from the agency and that you can claim it online. The body of the message will usually state that the IRS made an error in calculating your tax bill and now owes you money.

How can you tell it’s fake?
There are clues to alert you that this message is fake. The biggest, though, is the message itself. The IRS will never email you to ask for your personal information. If you get a message saying that the IRS owes you money, call the government agency yourself to check. The odds are high that the IRS doesn’t owe you anything and that a scammer sent you the message.


IRS

Claim Your Tax Refund Online

We identified an error in the calculation of your tax from the last payment, amounting to $ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

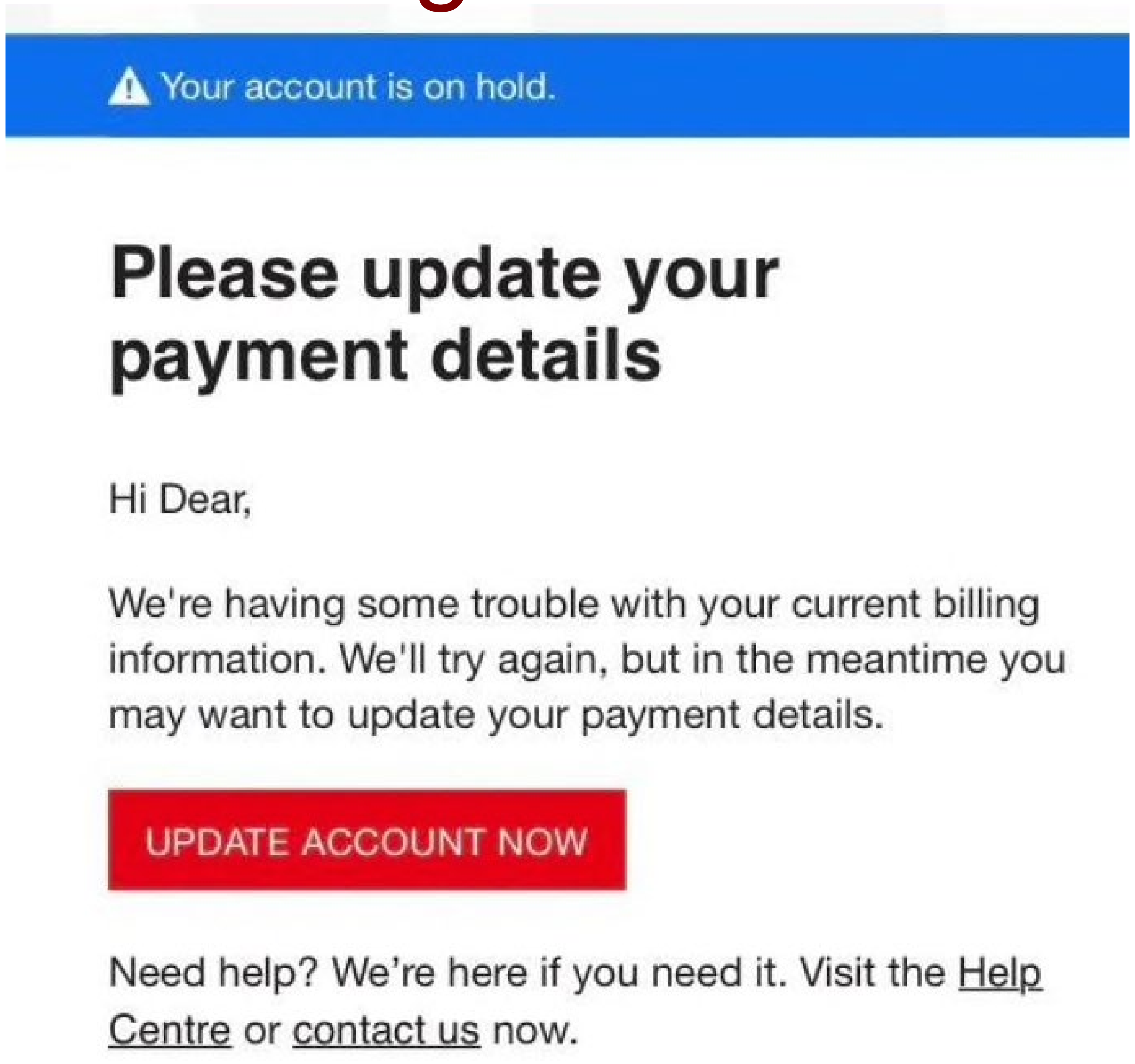
Phishing Example: Netflix Phishing Scam

Seeing an email claiming your Netflix account is on hold can be frightening. You never want your Netflix account to go down.

In this scam, criminals send an email, supposedly from Netflix, complete with the company's logo, saying that the company is having trouble with your current billing information. You're then asked to click on a link to update your payment method.

Also, pay attention to the language of emails like this. In this example, the scammers behind the email start their message with the salutation "Hi Dear." No business would address its customers in that way.

How can you tell it's fake?
Again, Netflix won't reach out to you through email to request your personal information. If you receive a message like this from Netflix, call the company directly to determine if you really do need to update your account.



⚠ Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

Need help? We're here if you need it. Visit the Help Centre or contact us now.

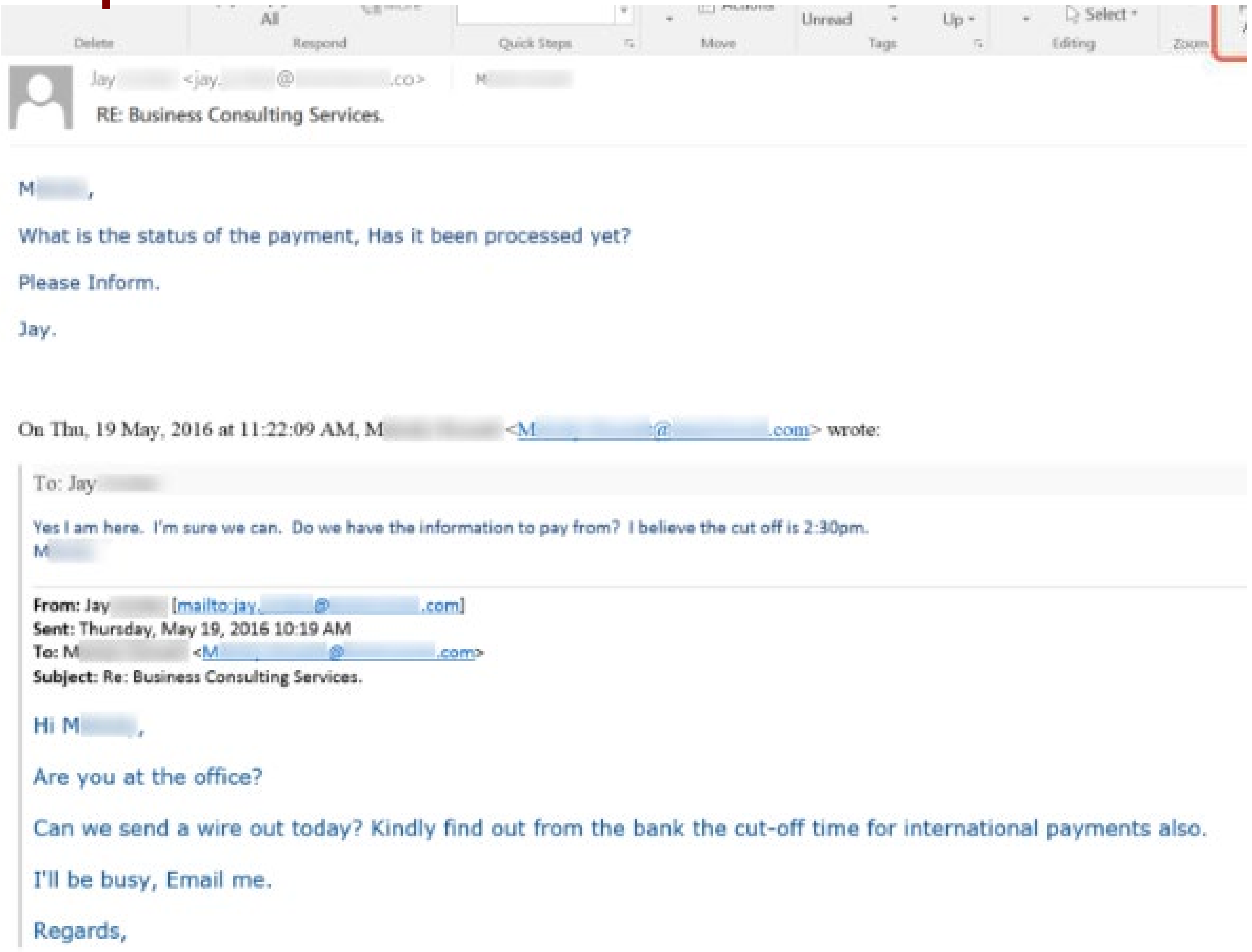
Phishing Example: CEO Fraud

Some phishing attempts have limited targets but the potential for big paydays for crooks. One example is the CEO phishing attempt.

Scammers send these emails to the employees of specific companies. These messages come from addresses that appear to belong to the CEO, CFO, etc. The email will ask the employee to wire money—often thousands of dollars—to a vendor or client. Only later does the employee realize that the message was a scam.

How can you tell it's fake?
CEO phishing emails are often sophisticated. You can look for misspellings or grammatical errors, but you might not spot any. You can check the email address of the sender, too. Often, it will be similar to the company's email format, but with a slight difference.

The biggest clue, though, that these messages are fake? Wouldn't your company's CEO or CFO ask you in person to send large sums of money and not rely on email wheen sending such an important request?



Jay [redacted] <jay.[redacted]@[redacted].co> M[redacted]
RE: Business Consulting Services.

M[redacted],

What is the status of the payment, Has it been processed yet?

Please Inform.

Jay.

On Thu, 19 May, 2016 at 11:22:09 AM, M[redacted] <M[redacted]@[redacted].com> wrote:

To: Jay [redacted]

Yes I am here. I'm sure we can. Do we have the information to pay from? I believe the cut off is 2:30pm.
M[redacted]

From: Jay [redacted] [mailto:jay.[redacted]@[redacted].com]
Sent: Thursday, May 19, 2016 10:19 AM
To: M[redacted] <M[redacted]@[redacted].com>
Subject: Re: Business Consulting Services.

Hi M[redacted],

Are you at the office?

Can we send a wire out today? Kindly find out from the bank the cut-off time for international payments also.

I'll be busy, Email me.

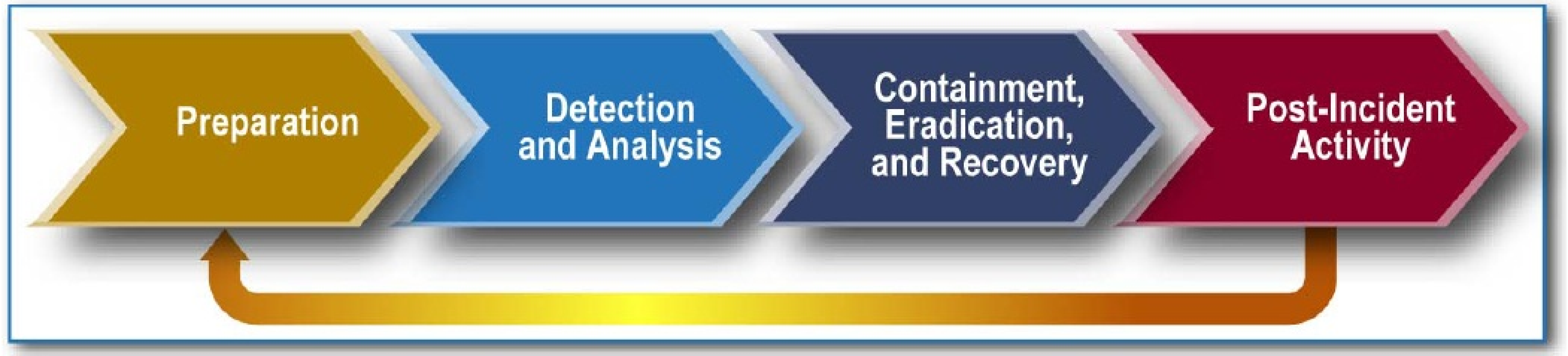
Regards,

What Goes in a Plan?

- **Scope**
  - Privacy-only incidents
  - Security-only incidents
  - Intersection of privacy/security

- **Team**
  - Manager + core team + others

- **Actions**
  - What needs to get done?



What Goes in a Plan?

- **Responsibility**
  - Who owns each action?
  - Clearly identify leaders

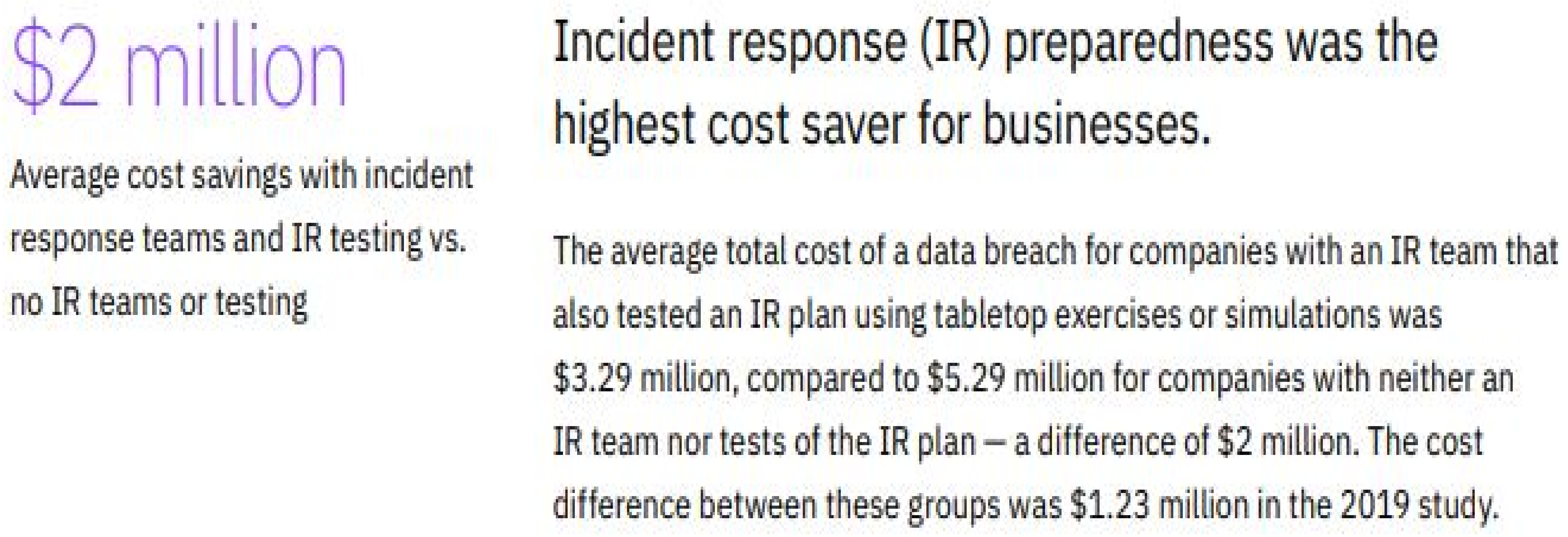
- **Risk framework—consider ENISA** *enisa.europa.eu/publications/dbn-severity*

- **Attorney–client privilege**
  - Be sure to involve Legal early

enisa
THE EU
CYBERSECURITY
AGENCY

Consider how and where you will track information related to an incident in a secure way that is accessible to the appropriate team members

Plans Save Money



$2 million

Average cost savings with incident response teams and IR testing vs. no IR teams or testing

Incident response (IR) preparedness was the highest cost saver for businesses.

The average total cost of a data breach for companies with an IR team that also tested an IR plan using tabletop exercises or simulations was $3.29 million, compared to $5.29 million for companies with neither an IR team nor tests of the IR plan — a difference of $2 million. The cost difference between these groups was $1.23 million in the 2019 study.

Key Vendors

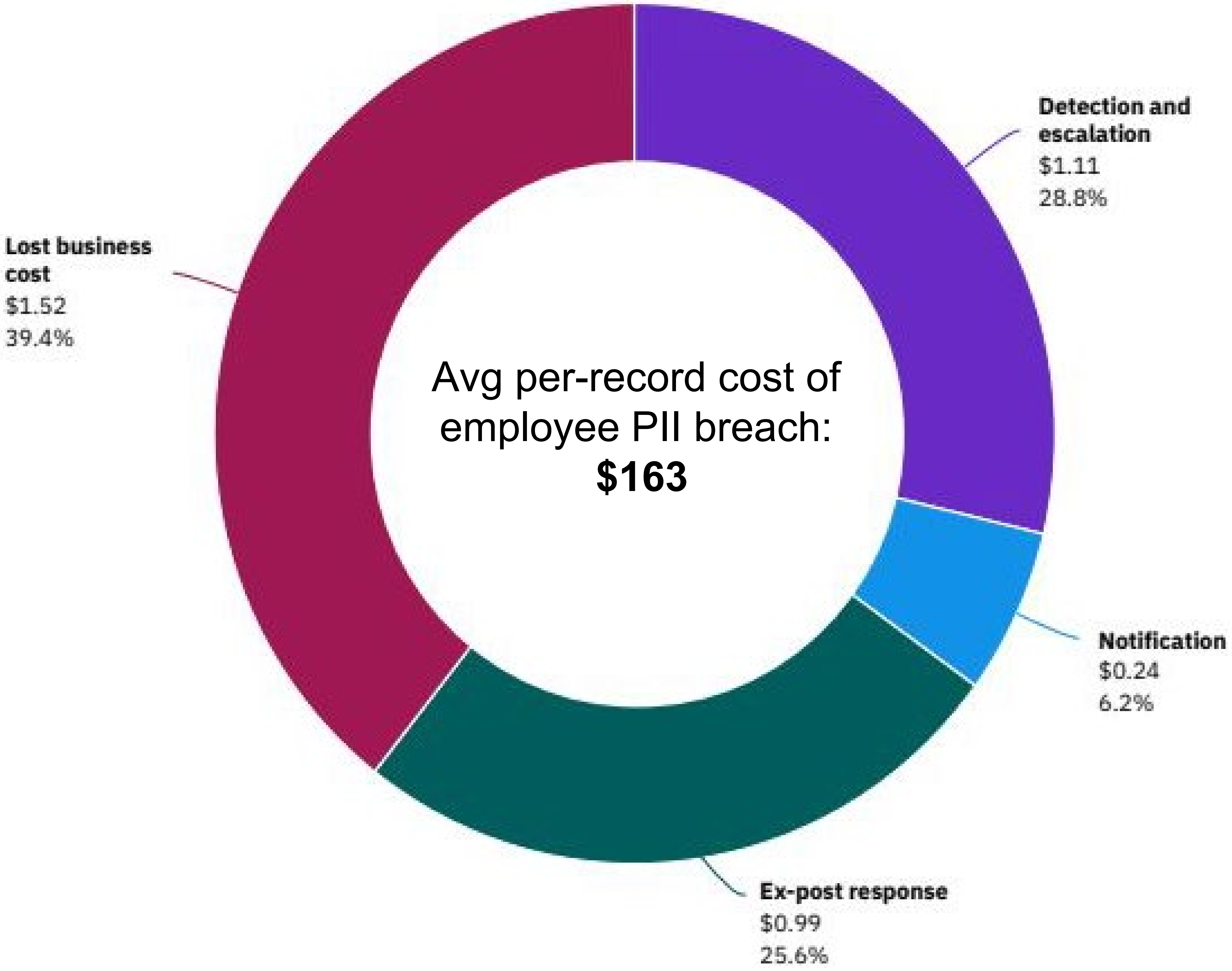
- **Forensics**
  - Speed matters!
  - Hire before you have an incident
- **Outside counsel**
  - Speed still matters!

Key Vendors

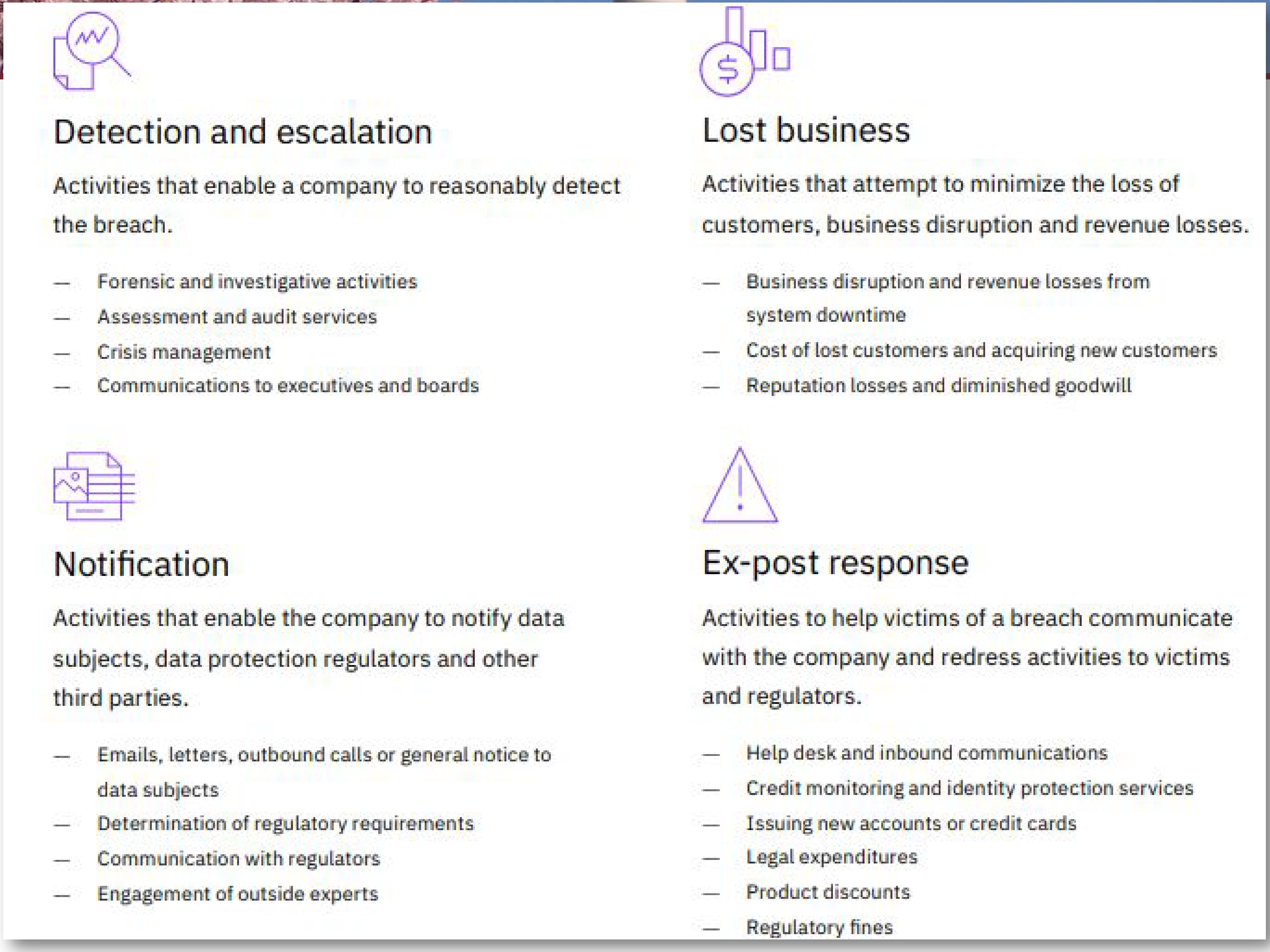
- **Public relations/communications**
  - Internal comms, external comms
- **Breach management services**
  - Print shop, call center, credit monitoring/identity theft protection
- **Cyber insurance**
  - Check for preapproved vendors, discounts with vendors, breach coach services, end-to-end breach response services
  - Know in advance who to call and who is permitted to call

Data breach average total cost divided into four categories

Measured in US$ millions



Avg per-record cost of employee PII breach: **$163**



Detection and escalation

Activities that enable a company to reasonably detect the breach.

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards

Notification

Activities that enable the company to notify data subjects, data protection regulators and other third parties.

- Emails, letters, outbound calls or general notice to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts

Lost business

Activities that attempt to minimize the loss of customers, business disruption and revenue losses.

- Business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill

Ex-post response

Activities to help victims of a breach communicate with the company and redress activities to victims and regulators.

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fines

© Randy Glasbergen / glasbergen.com

GLASBERGEN

“Should I arrest Clark Kent for identity theft or should Clark Kent have me arrested for identity theft? This is all so very confusing!”

Cyber or Privacy Insurance—Top 10 Reasons

1. Complying with breach notification laws costs time and money.
2. Third-party data is valuable, and you can be held liable if you lost it.
3. Data is one of your most important assets, yet it is not covered by standard insurance policies.
4. Systems are critical to operating your day-to-day business, but their downtime is not covered by standard business interruption insurance.
5. Cybercrime is the fastest-growing crime in the world, but most attacks are not covered by standard property crime insurance policies.
6. Retailers face severe penalties if they lose credit card data.
7. Your reputation is your No. 1 asset, so why not insure it?
8. Social media usage is at an all-time high, and claims are on the rise.
9. Portable devices increase the risk of a loss or theft.
10. It’s not just big business being targeted by hackers, but lots of small ones too.

OUR DEVICES ARE NOW 100% SECURE.
HOW DID YOU DO THAT?
I TURNED THEM ALL OFF.

© D.Fletcher for CloudTweaks.com

Risk Trends to Watch

Uncovered technology errors and omissions (E&O)

Covid-19 has accelerated digital transformation initiatives for many organizations. The emergence of technology services and product exposures in more traditional industries represents a potentially “new” E&O exposure that may not be contemplated by existing insurance.

Remote workforce

The remote workforce is here to stay, increasing potential vulnerabilities given remote desktop protocol (RDP) software, remote access security, reliance on third party IT service providers, and digital communication as the primary venue to share information.

Breach regulations

The regulatory environment continues to grow in complexity on a state, national and global basis. Recent fines under the European Union General Data Protection Regulation (GDPR), California Consumer Privacy Regulation (CCPA), and the Illinois Biometric Information Protection Regulation (BIPA), demonstrate that organizations should be mindful of the impact of a breach. Continued evolution in this space could bring larger financial concerns from a fines and penalties standpoint.

Cyber extortion

Theft and misuse of personally identifiable information (PII). Ransomware attacks have evolved to include not only the encryption of sensitive data (including PII and confidential corporate information), but also the threat of exposure of sensitive data on the public Internet. These types of attacks may result in corporate downtime due to encrypted networks as well as potential liability consequences in terms of regulatory fines or third-party lawsuits.

Vendor risk

As organizations continue to adapt to the current business environment and associated market needs, reliance on third-party technology and back-end applications has never been higher. Supplier cybersecurity standards are a critical part of this equation.

Cyber Insurance Snapshot

Key 2020 trends include:

Claim frequency—We saw a typical cadence of three new E&O/cyber matters per business day in 2020, **up almost 100%** from full-year 2019, the majority being ransomware event-related.

Claim severity—The average loss severity climbed each quarter of 2020. In many instances, **clients experienced eight-figure ransomware event-related losses**. Also, many of those large matters continue to be adjusted over the course of a year, as subsequent business interruption losses are reviewed and liability claims are litigated.

Pricing—While average pricing increased from 2019 to 2020 by 5%–10%, guidance from almost all insurers has been that those rate adjustments were not enough to compensate for the **increase in frequency and severity of losses. 2020–21—20–50% increase.**

Risk selection—Insurers bolstered supplemental tools throughout 2020. Some carriers are using public-facing scanning resources to search for vulnerabilities that could be subject to cyber threats, and many have introduced new ransomware-specific applications. These efforts are focused on **improving insured risk controls**, as well as **improving risk selection for insurers.**

Be a Better Risk—Recommendations

FOCUS ON: Cybersecurity

While no organization can eliminate the threat of a breach, being able to demonstrate basic steps to reduce the risk and significantly decrease the impact of a threat actor is critical. This requires proactive risk mitigation strategies, including assessment, testing, and practice improvement. It also requires incident response readiness, including conducting tabletop exercises and proactively retaining key third-party incident response providers. Leveraging resources available through an organization’s insurer partners may improve the outcome should a loss arise.

FOCUS ON: Privacy

Privacy maturity may be demonstrated via established and updated policies that address third-party contracts, online presence, service providers, supply chains, and each business unit. Emerging privacy regulations and requirements should be routinely reviewed with counsel, and insurance language should be reviewed to ensure it is broad enough to meet the evolving environment.

FOCUS ON: Cybersecurity culture

Employee cybersecurity and phishing training can demonstrate a culture of cybersecurity. No longer is this just an Admin/IT/Finance problem, employees should be trained to work to combat malicious actors and reduce common vulnerabilities. Without demonstrating adequate security training, insurers may struggle to provide competitive coverage terms or premium pricing.

FOCUS ON: Ransomware and business interruption

With carriers seeing both an increase in frequency and in severity of ransomware-related losses, companies should be prepared to showcase preparedness for a ransomware attack. Insurers are reviewing this exposure via specific questionnaires and use of scanning technology. Focus is on business continuity/disaster recovery planning, privileged access controls, multifactor authentication, proactive scanning/testing, and overall incident response readiness. This attack vector is of utmost concern to underwriters and will continue to transform the insurance market for the next several years.

FOCUS ON: Contracts

Third-party contracts are of consideration from a technology supply chain and contingent/dependent business standpoint. Critical supply chain and IT vendors are at heightened risk for “single point of failure” hacks impacting multiple organizations. It is critical to understand how both contracts and insurance respond in the case of a supply chain security breach.

Cyber Exposure

How long can your business operate without access to computer systems and the data they hold?

You are probably more dependent on computer systems than you realize. Understanding that modern businesses are partly or entirely reliant on technology in order to operate, cybercriminals increasingly see ransomware attacks and targeted extortion attacks as an easy way to make money. They do this by encrypting key data and demanding large sums of money in exchange for the decryption key. Most small businesses lack to the technical resources to deal with attacks like these in-house and may not have anyone experienced enough to turn to if their systems are brought down. Our incident response team notes that the average downtime is two to three days, but that's with the assistance of technical experts. In worst case scenarios, businesses aren't fully operable for weeks or even months after a cyber event. Backups are frequently targeted and disabled in these attacks, leaving businesses with little recourse when it comes to reinstating their data. Cyber insurance not only gives you access to a range of technical experts to help get you back online fast, but it also covers the financial losses incurred as a result of your business being interrupted and the costs of recreating any corrupted data. It can even cover the reputational impact of cancelled contracts and customers choosing to go elsewhere.

Do any of your employees work remotely?

Whether good practice or not, people reuse their passwords across multiple platforms, so if a username/password combination is breached in one cyber attack, hackers most likely have combinations for future attacks. With login credentials already to hand, cybercriminals can easily gain access to business email accounts or even log in to a company's remote desktop service (RDS). In addition, there's always the risk that work devices taken outside of the office can be lost or stolen. Cyber insurance can cover the fallout from hackers gaining access to your emails or systems, whether stolen funds, business interruption, or a privacy breach.

Are you confident that you or your employees will never make a mistake?

Humans are the weakest link in the cybersecurity chain. In fact, the vast majority of cyber incidents—for CFC, it's about 75%—involve some kind of human error or oversight. This includes everything from being tricked into giving over your username and password, reusing passwords(which makes account compromise easier), not following up wire transfer requests with a phone call, or losing devices containing sensitive information. Cyber insurance covers the financial losses that can result from these types of events as well as giving you instant access to the right specialists if someone makes a mistake. It also often comes with a range of free risk security tools and employee training.

Cyber Exposure

Do you send or receive wire transfer payments?

Cybercriminals are increasingly intercepting wire transfers, often by hacking into email accounts, pretending to be someone else, and sending fraudulent instructions. These scams are hard to spot because cybercriminals are taking the time to study how their victims send and receive payment requests, and they often come from real email addresses. Payments are rarely retrievable as they are siphoned off into other accounts quickly. Banks rarely refund the losses. Cyber insurance can refund the often-significant financial losses that come from scams like these. In fact, funds transfer fraud makes up about a quarter of CFC's cyber claims globally.

Do you collect or store personally identifiable information (PII) like credit card numbers or health information?

If sensitive information that you are responsible for is lost or stolen, you will most likely have to notify affected individuals of the breach and provide credit monitoring services. When it comes to PII, there are several rules and regulations about how you collect, use, and store that information. If you do not adhere to them, you could face regulatory fines and penalties. A malicious third party isn't always to blame. Often, it's as simple as an employee losing a company laptop. Cyber insurance covers the range of costs associated with data breaches, like notifying affected individuals and your responsibilities under different regulations. Even if you don't store PII, you probably store other business-critical information on your systems. See the next question to find out why this could pose a risk.

Do you store business-critical information on your computer systems, such as client contracts, designs and plans, stock levels, and other corporate information?

Even if you don't store a lot of customer records or credit card information, you still likely have important information that you need regular access to, from appointment bookings to intellectual property. What's more, if business-critical data becomes unavailable, it can have a serious impact on your ability to operate and ultimately your bottom line. See the next point for more information on business interruption.

Cyber Exposure: We Don’t Need Cyber Protection

We don’t need cyber insurance. We invest in IT security...

You’re still likely exposed. Not only are cyberthreats continually evolving to bypass the latest security measures, but even large corporations that spend vast amounts on cybersecurity still routinely get hit. People are still the weakest link in an organization's IT security chain. Approximately three-quarters of the cyber claims we deal with involve some kind of easily-preventable human error. Theft of funds, ransomware, extortion and non-malicious data breaches usually start with a human error or oversight such as leaving a laptop on a train or clicking on a phishing link, which then allows cybercriminals to access your systems from the inside. Cyber insurance is a cost-effective way to not only get access to risk management tools like phishing-focused employee training programs, but also to cover the financial loss if someone makes a mistake.

We outsource all of our IT, so we don’t have an exposure…

Unfortunately, using a third party for IT doesn’t eliminate your exposure. If you outsource your data storage to a third party and that third party is breached, you will still likely be responsible for notifying affected individuals and dealing with subsequent regulatory actions. What’s more, many businesses rely on third parties for business-critical operations, and should those providers experience a system failure, it could have a catastrophic effect on your ability to trade, resulting in a business interruption loss. Most third-party technology service providers have standard terms of service that limit their liability in the event that a breach or system outage causes financial harm to one of their clients.

We don’t collect any sensitive data, so we don’t need cyber insurance…

Two of the most common sources of cyber claims aren’t related to privacy at all—funds transfer fraud is often carried out by criminals using fraudulent emails to divert the transfer of funds from a legitimate account to their own, while ransomware can cripple any organization by freezing or damaging business-critical computer systems. Neither of these types of incidents would be considered a data breach, but both can lead to severe financial damage and are insurable under a cyber policy. Any business that uses technology to operate will have a range of other cyber exposures which a cyber policy can address.

Cyber Exposure: We Don’t Need Cyber Protection

Cyberattacks only affect big business. We’re too small to be a target…

Although cyber attacks affecting large organizations are most often in the news, over half of all cyber attacks are aimed at small businesses. This trend is continuing to rise. In 2018, attacks on small and medium-sized businesses rose by a staggering 424%. Cybercriminals see smaller organizations as low-hanging fruit because they often lack the resources necessary to invest in IT security or provide cyber security training. Cyber insurance is a great solution for smaller organizations because not only does it cover the growing number of cyber attacks on these businesses, but it gives you instant access to a number of technical and legal experts needed following a cyber event, but who you might not have in-house

Cyber is already covered by other lines of insurance…

Cyber cover in traditional lines of insurance often falls very short of the cover found in a standalone cyber policy. While there may be elements of cyber cover existing within traditional insurance policies, it tends to be only partial cover at best. Property policies were designed to cover your bricks and mortar, not your digital assets; crime policies rarely cover social engineering scams—a huge source of financial losses for businesses of all sizes—without onerous terms and conditions; and professional liability policies generally don’t cover the first-party costs associated with responding to a cyber event. A standalone cyber policy is designed to cover the gaps left by traditional insurance policies, and importantly, comes with access to expert cyber claims handlers who are trained to get your business back on track with minimum disruption and financial impact.

Cyber insurance is too expensive…

Cybercrime rates are quickly overtaking traditional crime rates, making cyber risk one of the most pressing business issues of today. For the sizeable losses you could be faced with—often in the hundreds of thousands—from stolen funds, lost revenue, or considerable cleanup costs, it is worth the extra insurance spend. Cyber insurance gives you instant access to a wide range of technical specialists who are experts at helping businesses quickly recover from cyber events. Policies also come with a range of free cybersecurity tools that you might spend hundreds or thousands on implementing yourself.

How to Prevent—Security Measures

- Information security policies—distributed to all employees (e.g., acceptable use, infosec, BYOD)
- Encrypt laptop hard drives
- Use two-factor authentication
- Use mobile device management to manage employee phones
- Require a VPN connection for remote access
- Security operations center—log/track security issues
- Use data loss prevention to prevent data from leaving your network
- Periodically run penetration tests on your network
- Use IP whitelists/blacklists
- Disable USB drives

Final Takeaways

- ❑ "Call Bob"—investigate cybersecurity coverage
- ❑ Top 10 reasons to obtain cybersecurity insurance handout
- ❑ Develop a customized incident response plan—see ENISA Framework = data breach severity methodology
- ❑ Be suspicious of everything!

More Info to Give You a Scare

- **Social engineering: Henderson Independent School District loses $600,000.00 in business email compromise (BEC) scheme: *youtu.be/BmlgtilTeio***

- **Denial of service: The Denial of Service Underground: DDoS Perpetrators and Attacks Exposed—YouTube**

- **Data breach: The 52 Biggest Data Breaches [Updated for 2021] | UpGuard**

CYBERSECURITY TEST

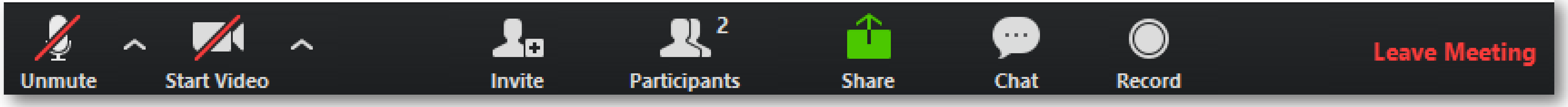
YES / NO

❑ ❑ Is Public Wi-Fi Safe?

❑ ❑ Should You Change Passwords Frequently?

❑ ❑ Do You Monitor Your Online Bank Account?

❑ ❑ Does Your Smartphone Have a Passcode?



ASA

2021 STAFFING LAW VIRTUAL CONFERENCE

APRIL 29–30

#staffinglaw