BUILDING INDUSTRY ASSOCIATION
of Philadelphia

How to Protect your Business From Cyberattacks

BRIAN VILE
President

VILETECH COMPUTER SOLUTIONS

JAY T. CROSBY, CRIS
Executive Director of Sales & Risk Solutions

EMMANUEL INSURANCE

8 Critical IT Security Protections EVERY Business Must Have In Place NOW

To Avoid Cyber Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties

BRIAN VILE

President, VileTech Computer Solutions

www.viletech.com

VILETECH COMPUTER SOLUTIONS

Today We're Going To Cover

1. The #1 security threat to your business that antivirus, firewalls and other security protocols can't protect against.
2. Why firewalls and antivirus software are not enough anymore.
3. 8 Security Protections You Can Implement Right Now To Better Protect Your Business

VILETECH COMPUTER SOLUTIONS

“But We’re Small… Nobody Would Bother To Hack Us, Right?”

Unfortunately, Wrong!

VILETECH
COMPUTER
SOLUTIONS

Half of all cyber attacks are aimed at SMBs.

(Source: Forbes Article, "5 Ways Small Businesses Can Protect Against Cybercrime")

VILETECH COMPUTER SOLUTIONS

Cybercrime by the numbers

2018: US $1.5 Trillion

2020: US $6 Trillion

Source:
Into the Web of Profit: Understanding the Growth of the Cybercrime Economy, by Dr. Michael McGuire.
World Economic Forums - http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

SECTION

01

The #1 security threat to your business that antivirus, firewalls and other security protocols can’t protect against.

VILETECH COMPUTER SOLUTIONS

It’s People!

VILETECH
COMPUTER
SOLUTIONS

Employee Training

Lack of an employee training program to raise awareness of cyber crime and cyber security.

VILETECH
COMPUTER
SOLUTIONS

65% of attacker groups used spear phishing as the primary infection vector

Source: Verizon Data Breach Investigations Report (DBIR) 2019

VILETECH COMPUTER SOLUTIONS

Phishing E-mail

From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

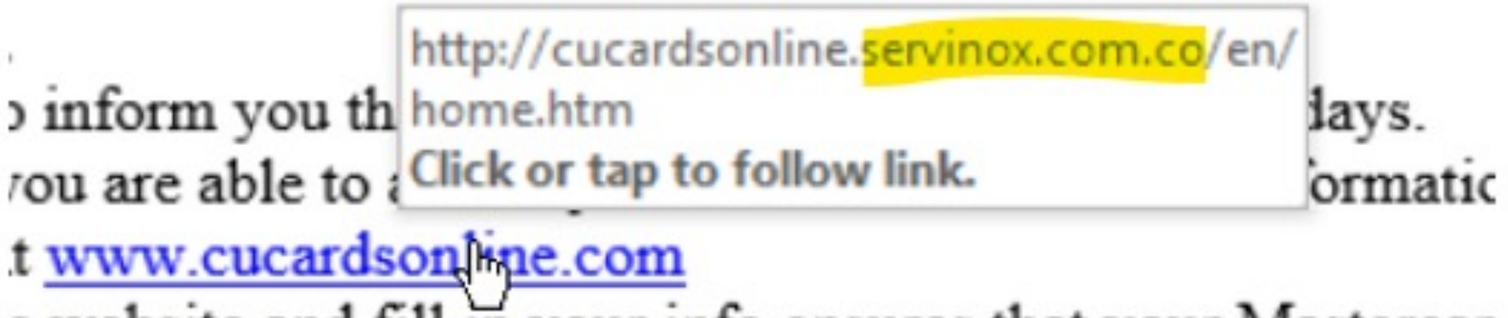
If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify..

Verify Now

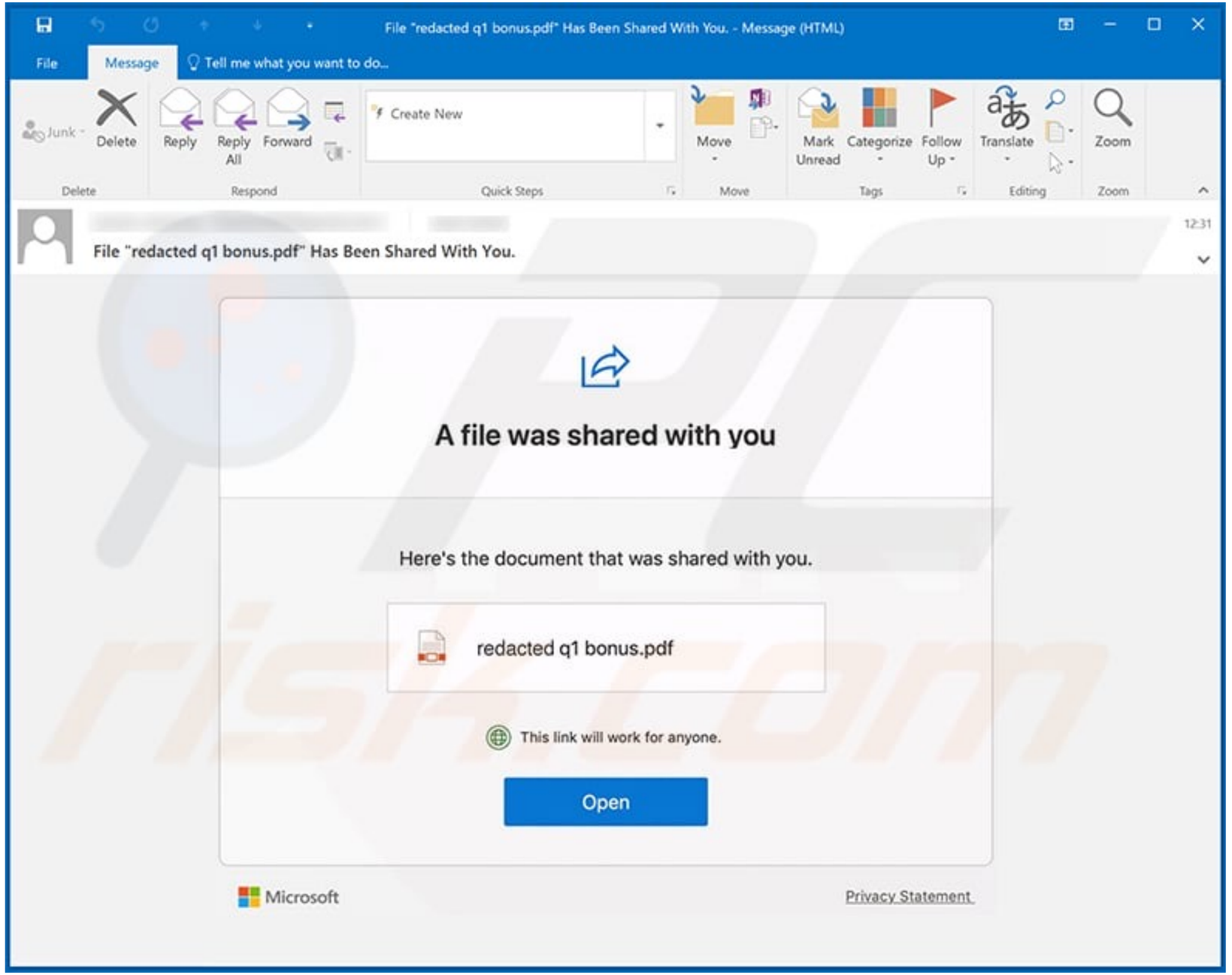
Microsoft Security Assistant
Microsoft office365 Team!

VILETECH COMPUTER SOLUTIONS

Spoofed URL



VILETECH
COMPUTER
SOLUTIONS



VILETECH COMPUTER SOLUTIONS

SECTION

02

Why firewalls and antivirus software aren’t enough anymore.

VILETECH
COMPUTER
SOLUTIONS


What is Zero Trust?

4 Ways Zero-Day Exploits Are Used In An Attack

Traditional security defenses like antivirus are developed to detect known malware. Zero-day exploits are extremely dangerous because unpatched vulnerabilities and unknown malware can go undetected for a long period of time. It is critical that you implement technology that will act as a barrier against zero-day exploits when they occur.

1 Phishing

A malicious actor or group sends fraudulent emails in order to lure recipients to a malicious or compromised website hosting an exploit.

2 Exploit Kits

A hacking toolkit used to take advantage of a software or application vulnerability. The functions available in these kits make it easy to distribute malware.

3 Spear Phishing

Cybercrimals use spear phishing to send files or other software executables that are embedded with a zero-day exploit.

4 Compromised System

Attackers can compromise a system, network, or server through brute-force and dictionary attacks or misconfigurations.

SECTION

03

8 Security Protections You Can Implement Right Now To Better Protect Your Business

VILETECH COMPUTER SOLUTIONS

Security Should Be Like An Onion

You have to have multiple layers of security before you get to the core.

VILETECH COMPUTER SOLUTIONS

PROTECTION

№1

Employee Education

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

№1

Implement An Employee Training Plan

We can make this easy.
Sign up each of your employees for our free security tip of the week.

www.VileTech.com/tips

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

№2

Require Strong Passwords and Passcodes To Lock Mobile Devices And Encrypt Them

VILETECH COMPUTER SOLUTIONS

PROTECTION

№2

Require Strong Passwords

- Especially Websites
- At Least 12 Characters Long
- Numbers, Symbols, Capitals
- Enable 2FA Everywhere Possible!!

VILETECH COMPUTER SOLUTIONS

PROTECTION

№2

Encrypt and Password Protect Mobile Devices

A PIN # and encryption keeps private data private.

VILETECH COMPUTER SOLUTIONS

PROTECTION

№2

Password Manager

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

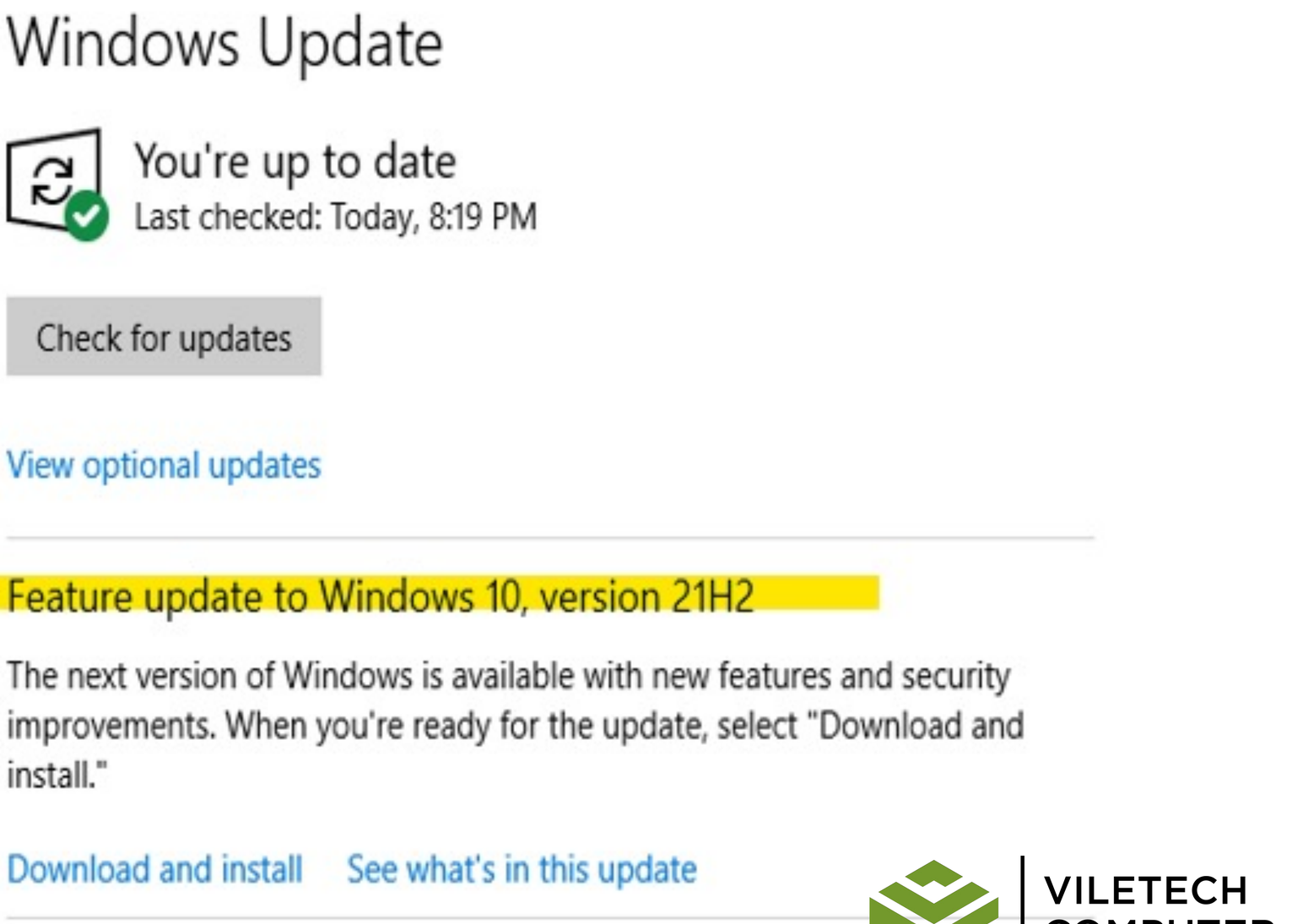
№ 3

Keep Your Network And Devices Patched And Up-To-Date

VILETECH COMPUTER SOLUTIONS

PROTECTION

№ 3



VILETECH COMPUTER SOLUTIONS

PROTECTION

№ 4

Have An Excellent Backup And Test It Regularly

VILETECH COMPUTER SOLUTIONS

PROTECTION

№ 4

Backup and TEST

Backup Daily

Send Offsite

Monitor Daily

Test At Least Monthly

Protects against accidental deletion, corruption, and ransomware

VILETECH COMPUTER SOLUTIONS

PROTECTION

№ 5

Encrypt your Data

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

№ 5

Windows 10
BitLocker

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

№6

Get A Solid UTM Firewall.

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

№6

Get One Built For Business Not A Home Router

VILETECH COMPUTER SOLUTIONS

PROTECTION

№6

Business Class Firewall

VILETECH COMPUTER SOLUTIONS

PROTECTION

№7

Spam Filtering

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

№ 7

Spam Filtering

Not Just A Spam Filter
Removes Viruses
Removes Phishing Attempts
Increases Productivity
Prevents malware

VILETECH
COMPUTER
SOLUTIONS

PROTECTION

№8

Control Which Websites Employees Are Accessing

VILETECH COMPUTER SOLUTIONS

PROTECTION

№8

Web Filtering

Block known malware sites before the computer loads the site.

Bonus: Block time wasting sites to boost productivity

VILETECH COMPUTER SOLUTIONS

Bottom Line

You Need To Get Serious
About Protecting Your Company
Against Cybercrime!

VILETECH
COMPUTER
SOLUTIONS

Cyber Insurance- A Look at Claims & Coverage

JAY T. CROSBY, CRIS

Executive Director of Sales & Risk Solutions, Emmanuel Insurance

www.emmanuelins.com

EMMANUEL INSURANCE

“There are two types of companies:
those who have been hacked, and those that will be.”

- Robert Mueller, FBI Director 2012

EMMANUEL
INSURANCE

Spencer House Apartment Complex in Beaverton, Oregon recently experienced a data breach involving physical files. Residents at an apartment complex blamed the apartment management for leaving their personal information out in the open. The documents were found in an unlocked public container that was sitting off a side street in their apartment complex. The documents included **Social Security numbers, addresses, phone numbers, immigration numbers and names.** It is vital to make sure your cyber policy covers paper breaches.

It is reported that Briggs Electric experienced a ransomware attack, known as Cryptolocker. They first noticed the problem when employees couldn't access files. Cryptolocker encrypted all of their Microsoft Word, PDFs, Excel files. It took Briggs Electric one full week to get back online, recover files, and clean up their machines. **Briggs Electric would have had to pay anywhere from $200 - $500 per hour for a forensic analysist to fix their systems.** Additionally, they lost profits after systems were down, delaying projects and rendering employees useless. All it takes is an employee accidentally clicking on a link containing malware for an attack like this to happen. Often times, hackers will demand a ransom as well to unlock files.

In March 2012, the Massachusetts Attorney General **fined a property management firm $15,000** after a company laptop containing unencrypted personal information was stolen. In addition to civil penalties the company was required to ensure that use of portable devices was limited, information stored on them was encrypted, and they were stored in a secure location. The company was also required to train employees on the policies and procedures for securing and maintaining the security of personal information.

Flooring Contractor (Revenue: <$1,000,000) - Wire Transfer Fraud

Puyallup, Washington

In 2019, a local contractor in Washington suffered a devastating wire transfer fraud attack. This business installed floors in residential and commercial buildings. One month, they were making a standard order from one of their trusted suppliers. The supplier mailed a physical invoice to the business owner. Shortly after, the contractor also received the same exact invoice, via email, providing wire transfer instructions and they paid, per usual. Two weeks later, the supplier followed up for their payment and it turns out the money was wired to a fraudulent bank elsewhere in the world. **The funds were not recovered, and the flooring contractor was out $50,000.**

Real Estate firms handle large sums of money every day as employees facilitate various wire transfers to several entities throughout the purchasing process. This makes real estate companies a prime target for **Social Engineering attacks**. Hackers often infiltrate email systems, monitor communications between employees and pose as home buyers or financial professionals in an attempt to convince employees to transfer funds into fraudulent bank accounts.

EMMANUEL
INSURANCE

An American real estate firm announced that an unauthorized third party gained access to their computer system. This computer system contained employee's personal information including **first and last names, addresses, Social Security numbers, usernames, and passwords**. Keller Williams was forced to notify every current or former associate whose information may have been compromised. Keller Williams also offered free year-long enrollment in Experian Credit monitoring services.

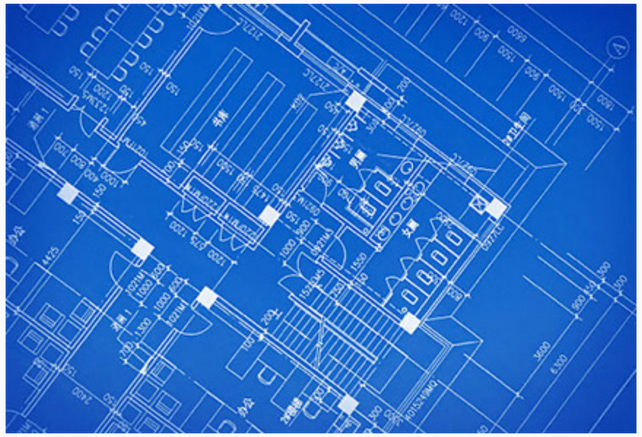
EMMANUEL INSURANCE

LARGE COMMERCIAL CONTRACTS

Did you know that an **HVAC contractor** was the reason for the 2013 Target breach that affected 41 million consumers? If you are performing work for large commercial organizations, you may have access to their networks, systems, and internal processes. This access can be exploited. When competing for a large commercial contract, a cyber policy is crucial because it will protect you and give you a competitive advantage.

CYBER & PRIVACY LIABILITY

Construction firms collect tons of sensitive information about their clients and ongoing projects. This data can include records of personally identifiable information, payment information, architectural plans, and even insight into a client's internal network. If this information is lost, **you are responsible for notifying the affected individuals and may face lawsuits, fines, and incredibly high forensics costs**.



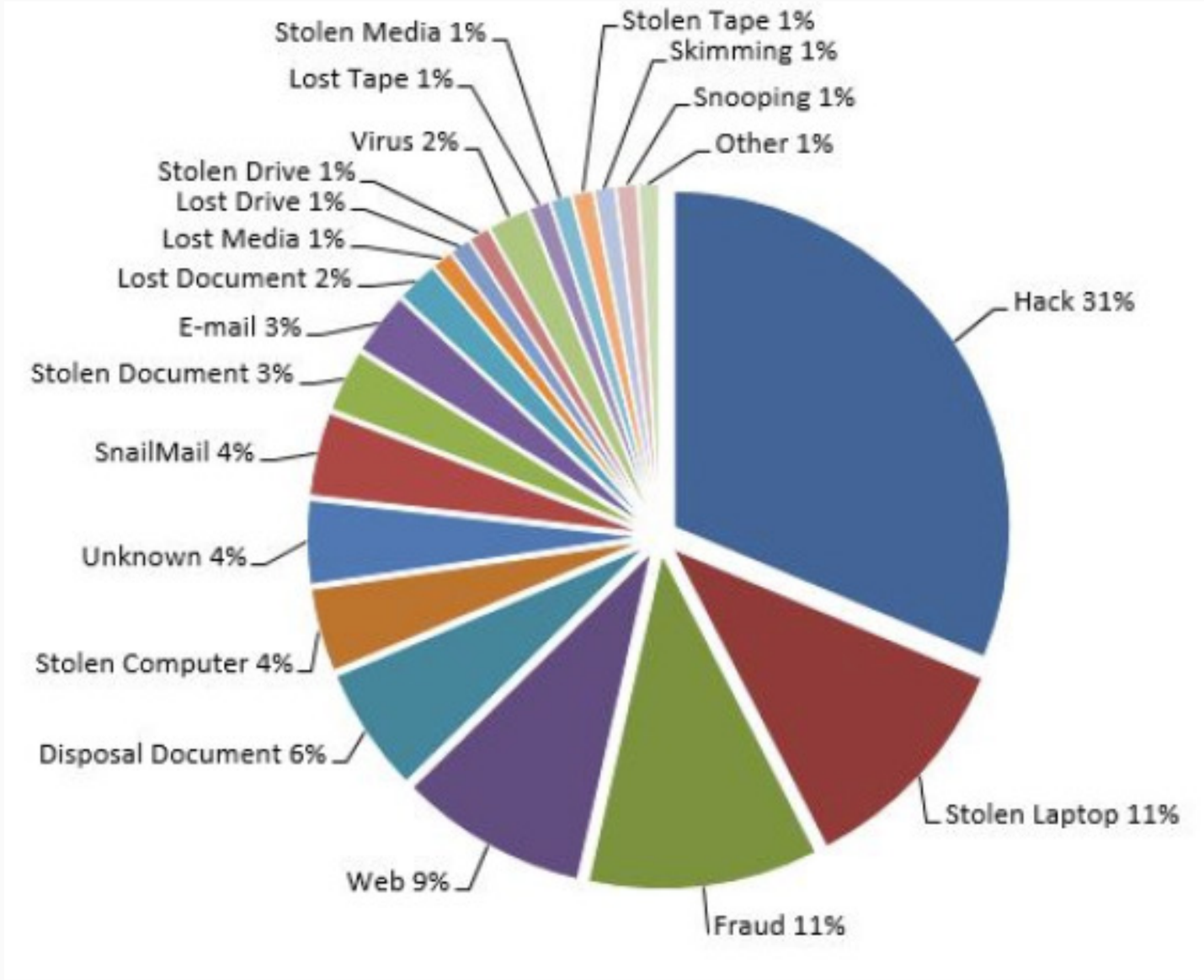
EMMANUEL
INSURANCE

BUSINESS INTERRUPTION

If your construction firm is relying on technology to run day to day operations, you need to make sure you have adequate Business Interruption coverage in your cyber policy. Are you using a laptop to track the progress of your job or strategically plan next steps and communicate with other individuals? If you can't access this information and connect with individuals involved on the project, **there is potential for a serious loss of profit.**

EMMANUEL INSURANCE

Sources of Breaches



Miscellaneous Crime Losses

A number of crime loss types do not fit neatly into any of the aforementioned categories. Examples of such losses:

- Defacing Web pages. Hackers download a firm's website and change pieces of information found within it, wreaking havoc with the company's business. However, they do so without actually stealing any information, merchandise, or funds.

- Intercepting e-mail Internet messages of a proprietary nature. A competitor gains access to a company's e-mail system and learns the date on which the company will introduce a new product. This allows the competitor to accelerate the introduction of its own competing product before its competitor's version is released.

- Posting embarrassing material. A hacker posts pornographic material on a newspaper's website. The newspaper incurs expenses and downtime to remove the hacked-in material.

Miscellaneous Crime Losses

- Posting source codes. A hacker penetrates the internal system of a software company and posts the details of its software product source codes on a website. The software company incurs costs to restore its system, as well as to find and bring a lawsuit against the responsible hacker.

- Sabotage by employees. A programmer for a magazine publisher is terminated from employment. During the evening of the day he is terminated, the employee enters the magazine's building and successfully logs onto its system. The former employee then deletes an entire issue of the magazine, and the publisher incurs substantial expenses to recreate it.

- Illegal system use by employees. A telecommunications company employee taps into the company's long-distance phone system and sets up a private, illegal, long-distance phone service. When finally discovered, the company incurs losses from lost billings as well as repair costs.

- Spamming. Spam is unwanted and unsolicited e-mail sent to another's computer system. A massive spam attack on a telephone company takes up so much space on the company's server that it produces a degradation in service, causing the system to crash.

Choosing a Carrier:

- A carrier should offer both 1st and 3rd party liability coverage
- Use a carrier that offers additional resources to prevent a breach
    - o Password protection software
    - o Employee training including phishing simulations
    - o Network Vulnerably Scan
- A carrier should use best in class breach response services
    - o Breach response vendors with a dedicated “Breach Coach” legal experts
    - o Multiple Forensics companies, notification and credit monitoring and public relations

EMMANUEL INSURANCE

Confusing Aspects of Cyber and Privacy Insurance Coverage

- The coverage is referred to by various names - it is not uncommon for one insurance company to have numerous cyber and privacy policy forms, each named differently.

  - ✓ Information Security and Privacy Insurance (Beazley)
  - ✓ CyberEdge (AIG)
  - ✓ CyberRisk and/or CyberFirst (Travelers)
  - ✓ Security and Privacy Protection (Zurich)
  - ✓ CyberSecurity (Chubb)
  - ✓ PrivaSure (AXIS Pro)
  - ✓ Enterprise Professional Solutions (CNA)

Confusing Aspects of Cyber and Privacy Insurance Coverage

- The coverage is referred to by various names - it is not uncommon for one insurance company to have numerous cyber and privacy policy forms, each named differently.
- It is often confused with technology E&O coverage.
- Both cyber and privacy and technology E&O policies cover many of the same risks.
- Both property and liability exposures are covered under cyber and privacy insurance.
- The nature of the coverage varies considerably from insurer to insurer.
- The menu-driven nature of the policies creates special problems.
- The cyber and privacy exposure is rapidly evolving.
- Cyber and privacy policies are also rapidly evolving.
- Cyber and privacy coverage aspects overlap with commercial general liability (CGL), professional, and media liability policies.
- Cyber and privacy forms contain a number of idiosyncrasies.

13 Steps To Reduce Cyber and Privacy Loss Exposures

- Centralize responsibility for data security.
- Fill out an application for coverage.
- Have a cyber audit by an outside firm.
- Monitor and manage outside service providers.
- Get a handle on laptops, mobile phones, and other portable electronic devices.
- Develop and test an incident response plan.
- Train employees on how to spot “phishing” attempts.
- Encrypt data.
- Design systems to handle higher-than-normal volumes of data.
- Secure servers.
- Limit online data collection.
- Use liability disclaimers.
- Employ e-mail security techniques.

EMMANUEL INSURANCE

The 13 Types of Insuring Agreements within Cyber and Privacy Policies

There are 13 different insuring agreements typically contained within cyber and privacy policy forms:

Coverage Type	Insuring Agreement
First-Party/Post Breach Response Coverage	1. Privacy Notification and Crisis Management Expense
Third-Party/Liability Coverages	2. Information Security and Privacy Liability 3. Regulatory Defense and Penalties 4. Payment Card Industry Fines and Assessments 5. Website Media Content Liability 6. Bodily Injury and Property Damage Liability
First-Party/Time Element Coverages	7. Business Interruption 8. Extra Expense
First-Party/Theft of Property Coverages	9. Data Assets 10. Cyber Extortion 11. Computer Fraud 12. Funds Transfer Fraud 13. Social Engineering/Fraudulent Instruction Coverage

EMMANUEL INSURANCE

Example of a cyber quote for GC that does $5M in Revenue

Policy Form and Endorsements: (see table to determine applicable endorsements per option)

- CY4000 Risk e-Business Cyber Loss & Liability Insurance Policy
- CY6000 Declarations for Risk e-Business Cyber Loss & Liability Insurance Policy
- CY7002 Disclosure Pursuant to Terrorism Risk Insurance Act
- IL7324 Economic and Trade Sanctions Clause
- CY1077 Ransomware Sublimit Endorsement ($100,000)
- CY0001 Service of Process Endorsement
- CY3005 Loss of Income Due to Negative Publicity
- CY3008 Separate Limits of Insurance for Loss Expense and Liability Expense

Plus applicable state amendatory endorsements (if any)

	Carrier: Great American Fidelity Insurance Company	
	Option 1 (E&S)	**Option 2** (E&S)
1st Party Limit	$1,000,000	$1,000,000
3rd Party Limit	$1,000,000	$1,000,000
Limit Type	Separate	Separate
Deductible	$5,000	$10,000
Waiting Period	Ten hours	Ten hours
Optional Coverage	Data Restoration ($1,000,000) Contingent BI ($250,000) CyberCrime ($250,000) Negative Publicity($250,000)	Data Restoration ($1,000,000) Contingent BI ($250,000) CyberCrime ($250,000) Negative Publicity($250,000)
Premium	$3,027.00	$2,885.00
Agency Fee	$75.00	$75.00
E&S Tax	$90.81	$86.55
Stamping Fee	$20.00	$20.00
Total	$3,212.81	$3,066.55

EMMANUEL INSURANCE

EMMANUEL
INSURANCE

www.emmanuelins.com