

What Can You Do to Prepare for the Next Cyber Attack?

Peace of mind is a matter of choice.

October 13, 2021

*Presented By:
Antonina McAvoy, CISA
Senior Manager*



What Can You Do to Prepare for the Next Cyber Attack?

Andrea P. Sardone
Today's Moderator



ARE YOU LEAVING THE DOOR OPEN TO CYBER CRIMINALS?



When your website is down, you can't serve your customers or meet service level agreements... and data has been compromised – that's a serious problem.

- Electric doorways we want sealed can be blown open.
- Two key takeaways:
 1. They may not be after only you.
 2. Your size simply does not matter.

```
int nblocks;
int i;

nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
/* Make sure we always allocate at least one indirect block pointer */
nblocks = nblocks ? 1;
group_info = kmalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
if (!group_info)
    return NULL;
group_info->groups = gidsetsize;
group_info->nblocks = nblocks;
atomic_set(&group_info->usage, 1);

if (gidsetsize
    group_info
else {
    for (i =
        gid_t
        b = 1;
        if (!b)
            goto out_undo_partial_alloc;
        group_info->blocks[i] = b;
    }
}
return group_info;

out_u|
```

ACCESS GRANTED

WILL A CYBER ATTACK DRIVE YOU OUT OF BUSINESS?

- 60% of companies hit do not recover.
- Attacks up 60% during and post-pandemic.
- Avg. Ransomware payment in 2021 increased 82% year over year to \$570,000.



62% of **cyberattacks** target small and mid-size businesses

CYBER ATTACKS MAKING HEADLINES

<https://www.cbsnews.com/news/jbs-ransom-11-milli...>

JBS paid \$11 million ransom after cyberattack - CBS News

Jun 10, 2021 — The world's largest meat processing company said Wednesday that it paid an \$11 million ransom to **cybercriminals** after it was forced to halt ...

<https://www.cnbc.com/2021/06/08/colonial-pipeline-c...>

Colonial Pipeline paid \$5 million ransom one day after ...

Colonial Pipeline paid \$5 million ransom one day after **cyberattack**, CEO tells Senate · The president and CEO of the **Colonial Pipeline** Co. · Joseph ...

<https://www.forbes.com/leemathews/2021/03/21/a...>

Acer Faced With Ransom Up To \$100 Million After Hackers ...

Mar 21, 2021, 12:23pm EDT |15,864 views ... **Cybersecurity** experts who spoke with Bleeping Computer recently observed a bad actor targeting an **Acer** Exchange ...

<https://www.securitymagazine.com/articles/95245-in...>

Insurance giant AXA victim of ransomware attack | 2021-05-19

May 19, 2021 — **AXA** said on Sunday that the **cyberattack** has targeted its Asia Assistance division, impacting IT operations in Thailand, Malaysia, ...

<https://www.businessinsurance.com/article/STORY>

Brenntag pays over \$4 million ransom to retrieve stolen data

May 14, 2021 — **Cyber**. German chemical distributor **Brenntag** SE reportedly paid a \$4.4 ... ransomware **attack** on the company, Bleeping Computer reported.



<https://www.cnn.com/2021/08/18/tech/t-mobile-data...>

T-Mobile says data breach affects more than 40 million people

Aug 18, 2021 — (CNN) Tens of millions of current, former or prospective **T-Mobile** (TMUS) customers' personal information has been leaked to hackers, ...

<https://thecybernewsfeed.com/cyber-alerts/data-brea...>

Data breach at US waste management firm exposes employees ...

Data breach at US waste management firm exposes employees' healthcare details. admin. August 12, 2021. 0 Comments. **Waste Management** Resources is ...

J&M CASE STUDY

General Information

J&M Tank Lines, Inc.

- Based in Birmingham, AL
 - 525 Employees
 - 420 Trucks
 - 871 Tanks
 - 11 Terminals
 - 120,000 loads delivered / year
- Highly Automated
 - 1 Payroll Clerk
 - 2 Billing Clerks
 - 1 AP Clerk



J&M CASE STUDY

Timeline of Events

What is YOUR maximum tolerable downtime?

Tuesday, April 2, 2019 [2:30AM] – Notification from CFO of RYUK Ransomware Attack Demanding \$250,000 in Bitcoin.

Tuesday, April 2, 2019 [8:30AM] – Reported incident to FBI - Referred to tech vendor. 3 vendors assisting J&M. Can't process paychecks due at end of the week or invoice customers.

Saturday, April 6, 2019 [5:00AM] – 1.75 Billion lines of data. Main system is up, but no sub systems.

Monday, April 8, 2019 [Day] – 1st freight bills cut.

2 weeks from this day until all sub-systems up and running.

Tuesday, April 2, 2019 [5:30AM] – Regained control of phone and e-mail systems back. Continuous back-up compromised. Estimated for system to be up at 11:30AM.

Tuesday, April 2, 2019 [1:00PM] – Problem with data in system – need to back-load a week's worth of data, and have a problem with one backup system. 4th vendor is brought in. Payroll double pay from week prior. Estimated up time 8AM April 4th.

Sunday, April 7, 2019 [Evening] – Caught up on data entry on Sunday PM.

Sunday, June 2, 2019 [3:30AM] – CFO calls – struck again. 60 days from the initial attack, system crashed again as hackers had installed a shut-down switch. FBI alerted of attack.

J&M CASE STUDY

Lessons Learned

If you're hit, the hacker has probably already been 'in' for a while. They can check your financials and see what you can afford to pay.

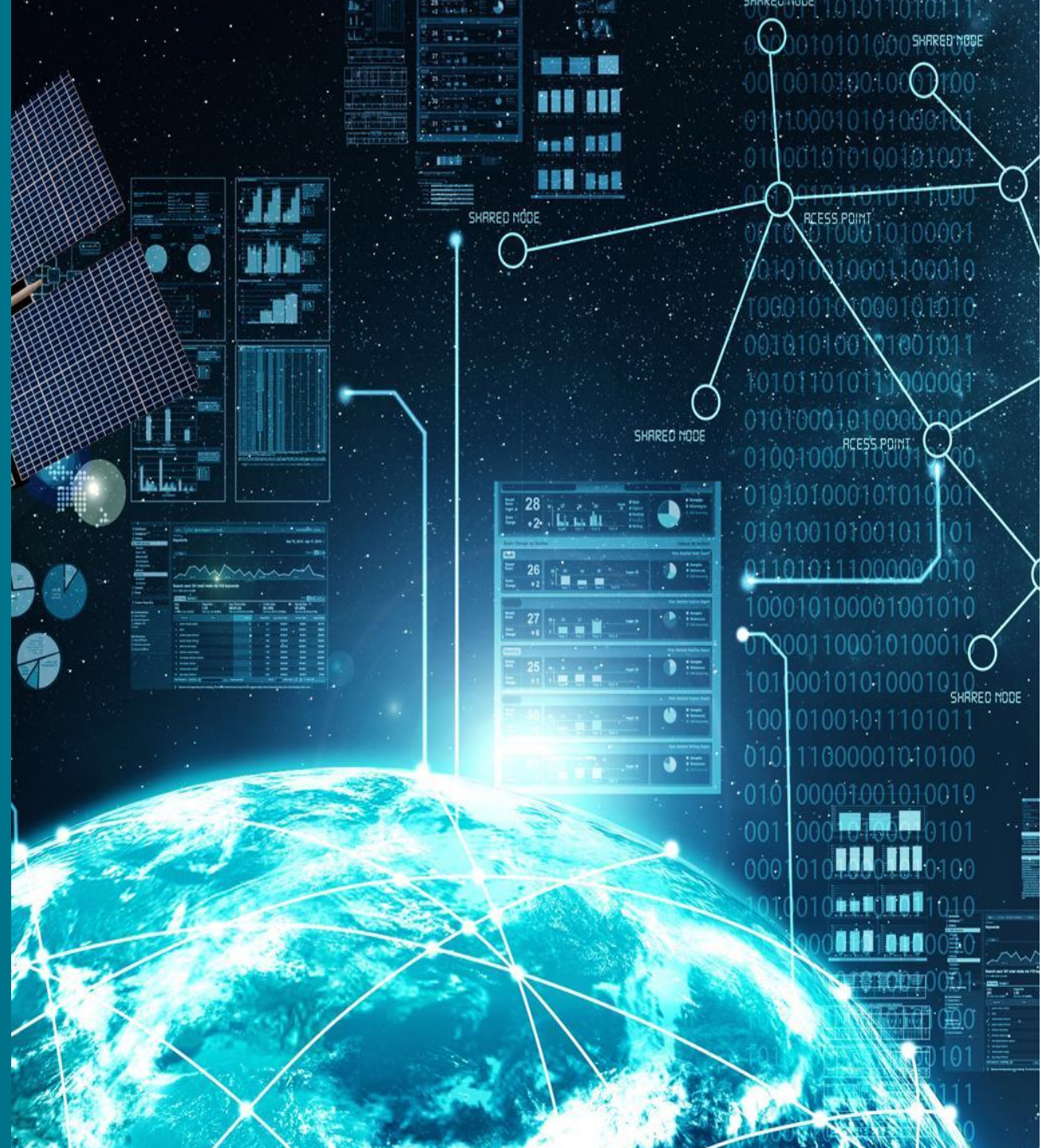
J&M Assembled a Team of Experts

- Law Firm: Specializes in cyber issues (contracts – shippers – vendors).
- Tech Team: Dual authentication implementation, three sets of backups, and move anything offline that can be moved offline.

What J&M has done to prevent this?

- CrowdStrike endpoint protection, threat intelligence, and cyberattack response services
- Cybersecurity training
- Dual authentication
- IronScales e-mail security
- Severely restricted Internet, program & resource access

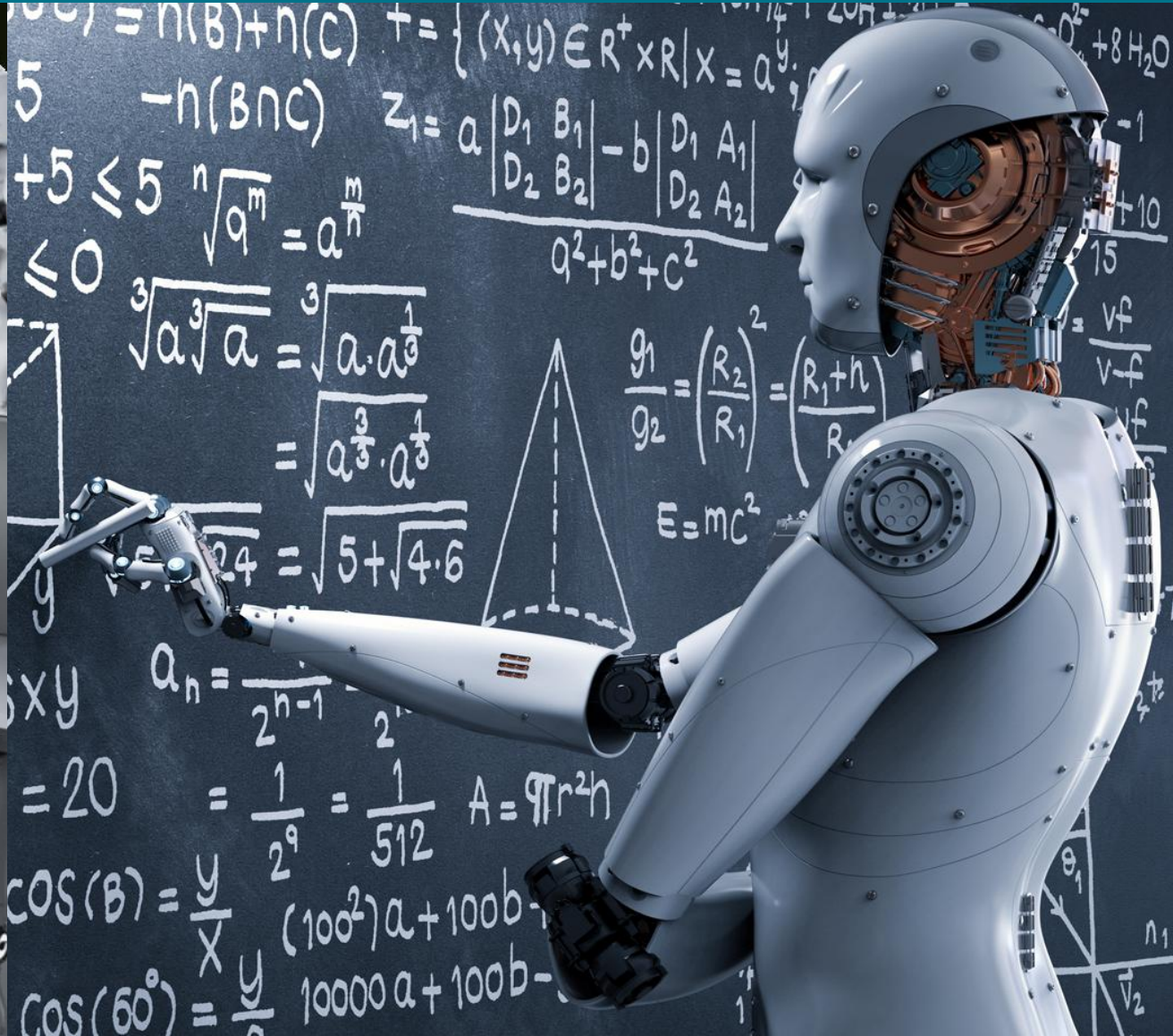
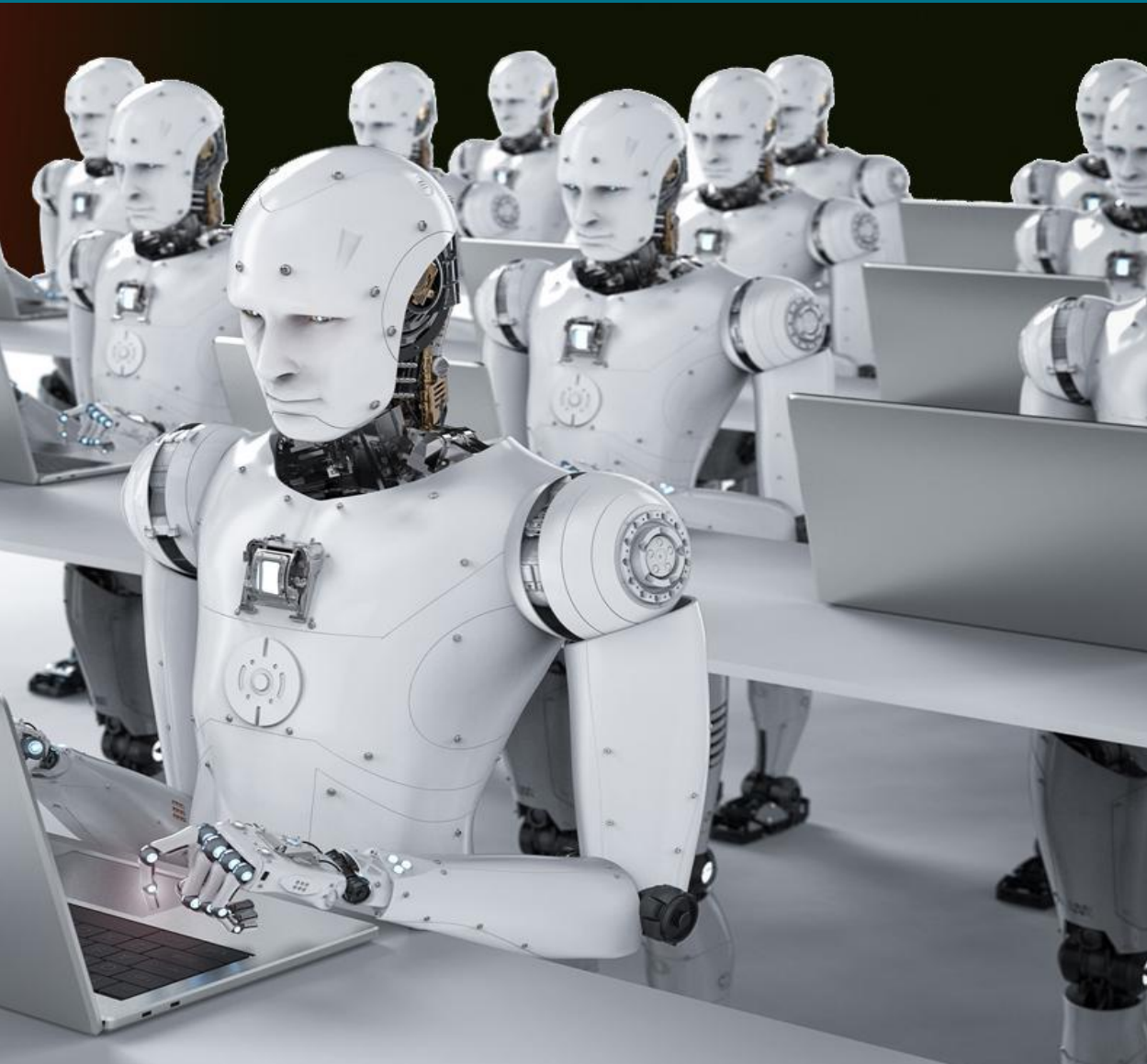
Global Cyber Warfare



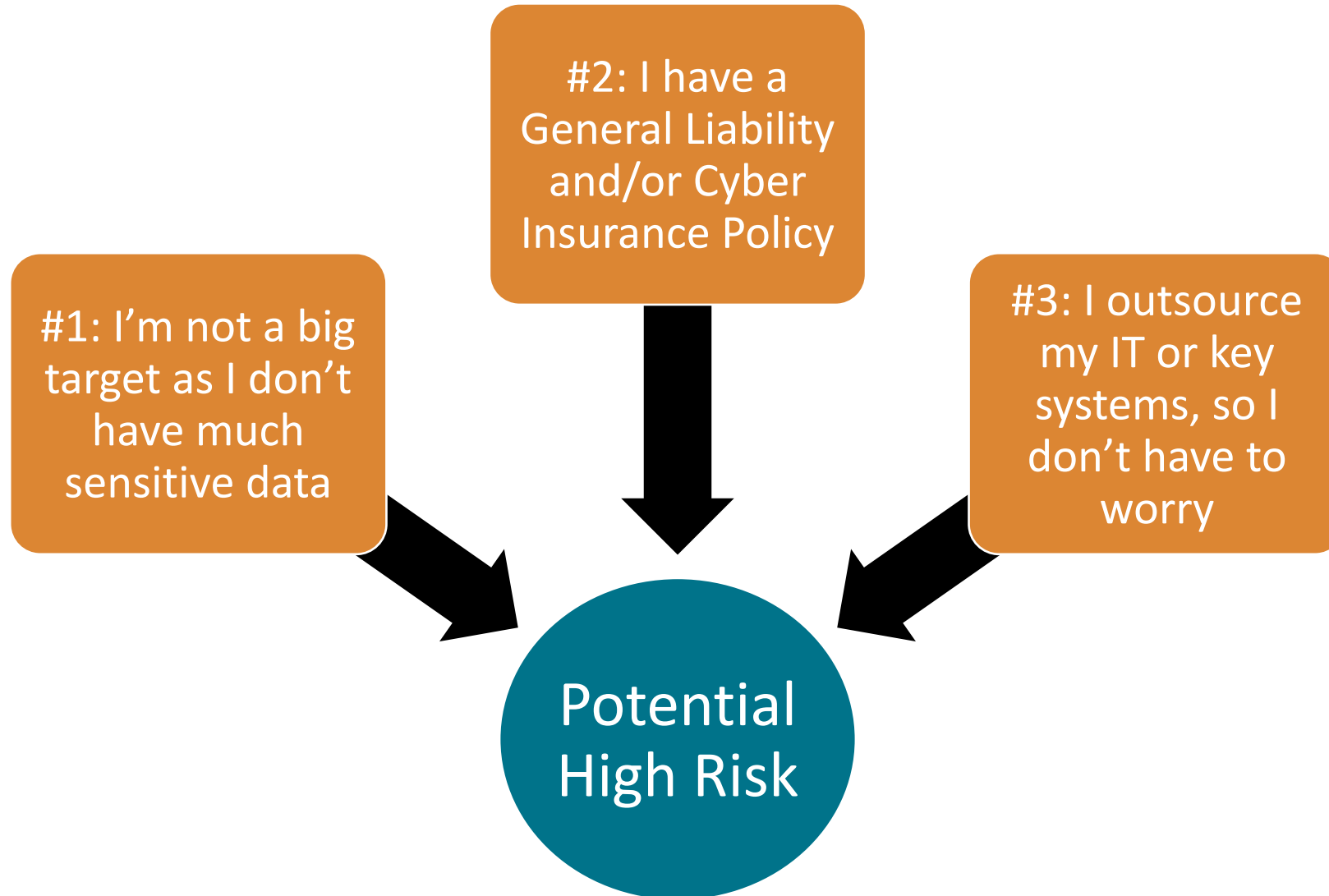
CURRENT STATE WE LIVE IN



ARMY OF ROBOTS

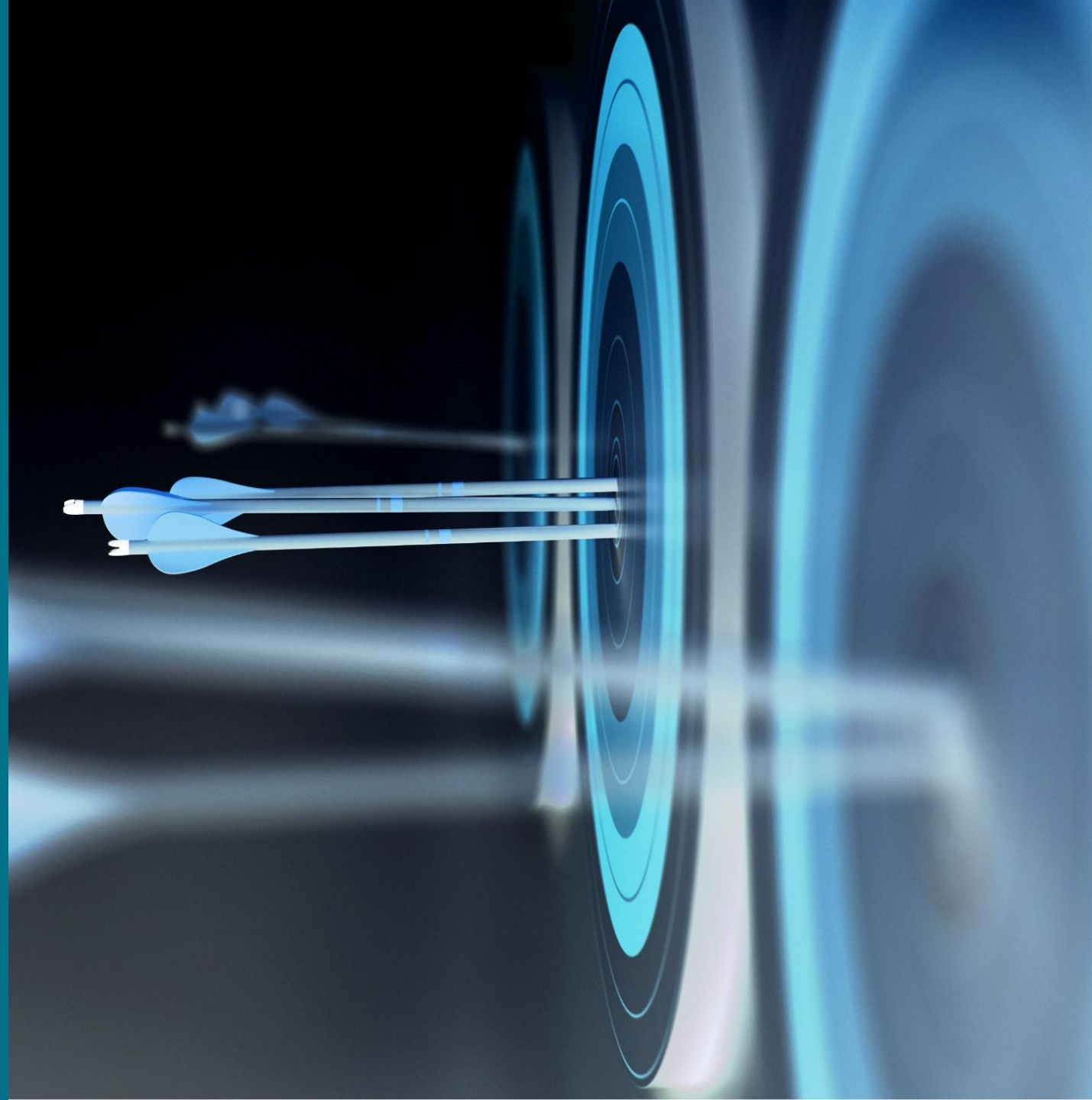


COMMON MISCONCEPTIONS



Misconception #1

I'm Not
a Big Target
as I Don't
Have Much
Sensitive Data.



DATA IS THE NEW OIL

**Employee
Data**

Credit Card Data

**Business
Correspondence**

**Confidential
Pricing Data**

**Electronic
Signatures**

**Customer
Lists**

**Trade
Secrets**

**Financial
Data
Records**

**Intellectual
Property**

**System
Connections**



TOP 5 CYBERATTACK METHODS



Ransomware Attacks

Denial of
Service (DDoS)
Attacks

Phishing
Attacks via BEC

Remote Desktop
Services (RDP)
Attacks

Password
Attacks

Misconception #2

I Have a
General Liability
and/or
Cyber Insurance
Policy.



HOW TO CHOOSE A CYBER INSURANCE POLICY?

Chubb?

AXA?

Liberty Mutual?

Corves?

Berkshire Hathaway Group?

Travelers?

Cowbell Cyber?

CNA?

Beazley?


Hiscox?

AIG?

Allianz?

Resilience?

COMMON REASONS CYBER INSURANCE APPLICATIONS ARE DENIED



Are you ready?

1. Inadequate cybersecurity testing procedures and audits.
2. Inadequate cyber incident response plans
3. Inadequate backup processes and recovery procedures.
4. Inadequate policies concerning the security of vendors and business partners
5. Inefficient processes to stay current on new releases and patches.
6. Poor-quality security software and employee training
7. Lack of adherence to a published security standard
8. Lack of use of multi-factor authentication

CASE STUDY: CYBER INSURANCE DENIED



BUSINESS INSURANCE.

Bank, insurer fight over coverage for cyber attack

- National Bank of Blacksburg v. Everest National Insurance Co.
- Hacked twice in less than a year and suffered total losses of \$2.4 million (phishing scam)

Not all policies are created equal. Do your homework and work with your broker in order to negotiate the best cyber insurance policy.

CYBER INSURANCE INDUSTRY TRENDS

<https://www.washingtonpost.com> › 2021/06/17 › ranso... ⋮

Ransomware attacks are pushing up the cost of cyber insurance

Jun 17, 2021 — **Cyber insurance** carriers are raising premiums and limiting **coverage** in the face of severe ransomware **attacks**.

1. Cyber insurance market to see rapid growth.
2. Pricing is going up
 - Premiums up 29%
3. Renewal applications are 25 questions instead of 4.
 - High emphasis on minimum security requirements – such as MFA, etc.
4. Cyberattacks are constantly evolving, making exposure difficult to anticipate.
5. Some insurers cautiously offering modest limits for restricted coverage.

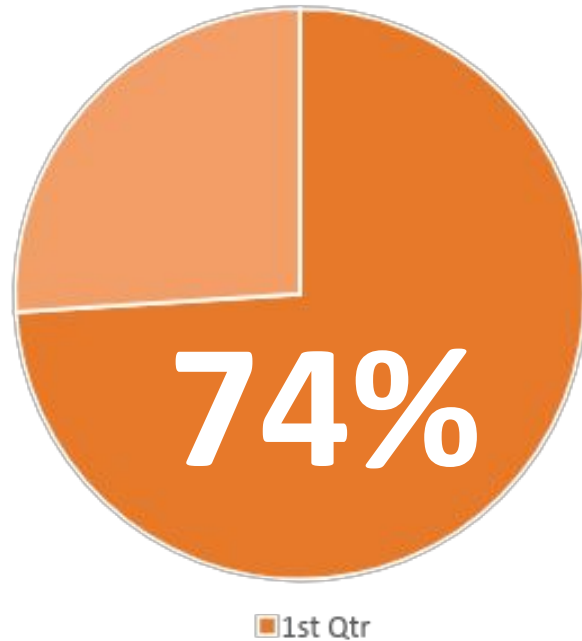
Misconception #3

I Outsource My IT
or Key Systems,
So I Don't Have
to Worry.



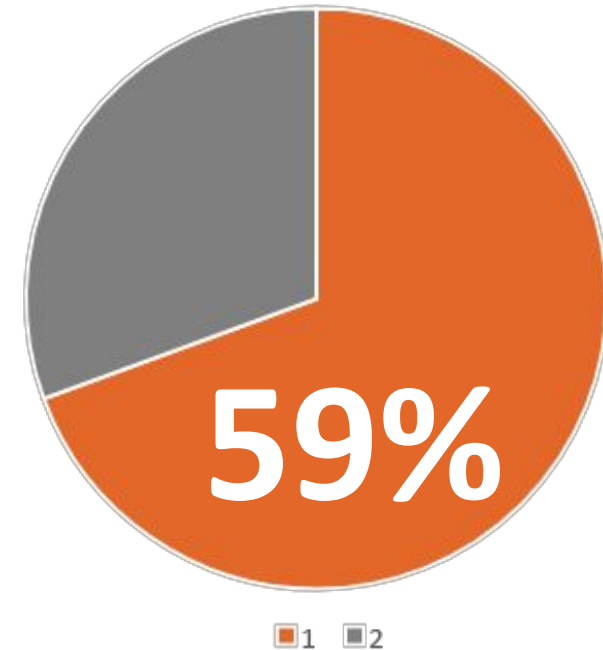
THIRD-PARTY VENDOR RISK

DELOITTE SURVEY



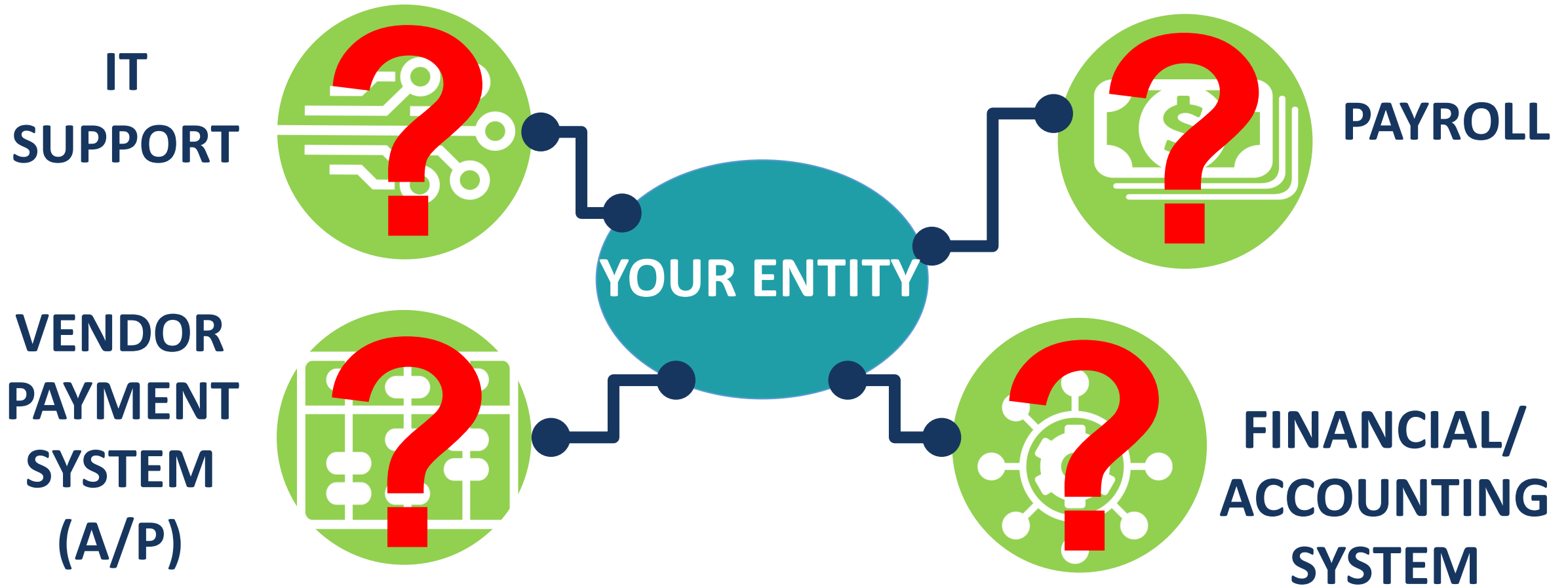
**THIRD PARTIES PLAY A CRITICAL
ROLE IN BUSINESS FUNCTIONS**

PONEMON INSTITUTE



**DATA BREACHES CAUSED BY A
THIRD-PARTY VENDOR**

CAN YOU RATE YOUR VENDOR'S RISK LEVEL?



Do you know who your weakest link is?

THE BLAME GAME





An Ounce
of
Prevention

CYBERSECURITY RISK IMPACTS YOUR WHOLE ENTITY



**EMPLOYEES
DRIVERS
CUSTOMERS
IT
OPERATIONS**

HOW CAN YOU MINIMIZE BEING A STATISTIC?



“A lot of transportation companies may have underinvested in cybersecurity. Bay & Bay was no different. You take it for granted and think that it’s not going to happen to you.”

Wade Anderson, Bay & Bay Transportation chief information officer



Key Consideration:

- What are your assets?
- What are your threats?
- What are your vulnerabilities?

ADDRESSING HUMAN ERROR

One employee, **one** click....that's all it takes

95% of **cyberattacks** are caused by human error

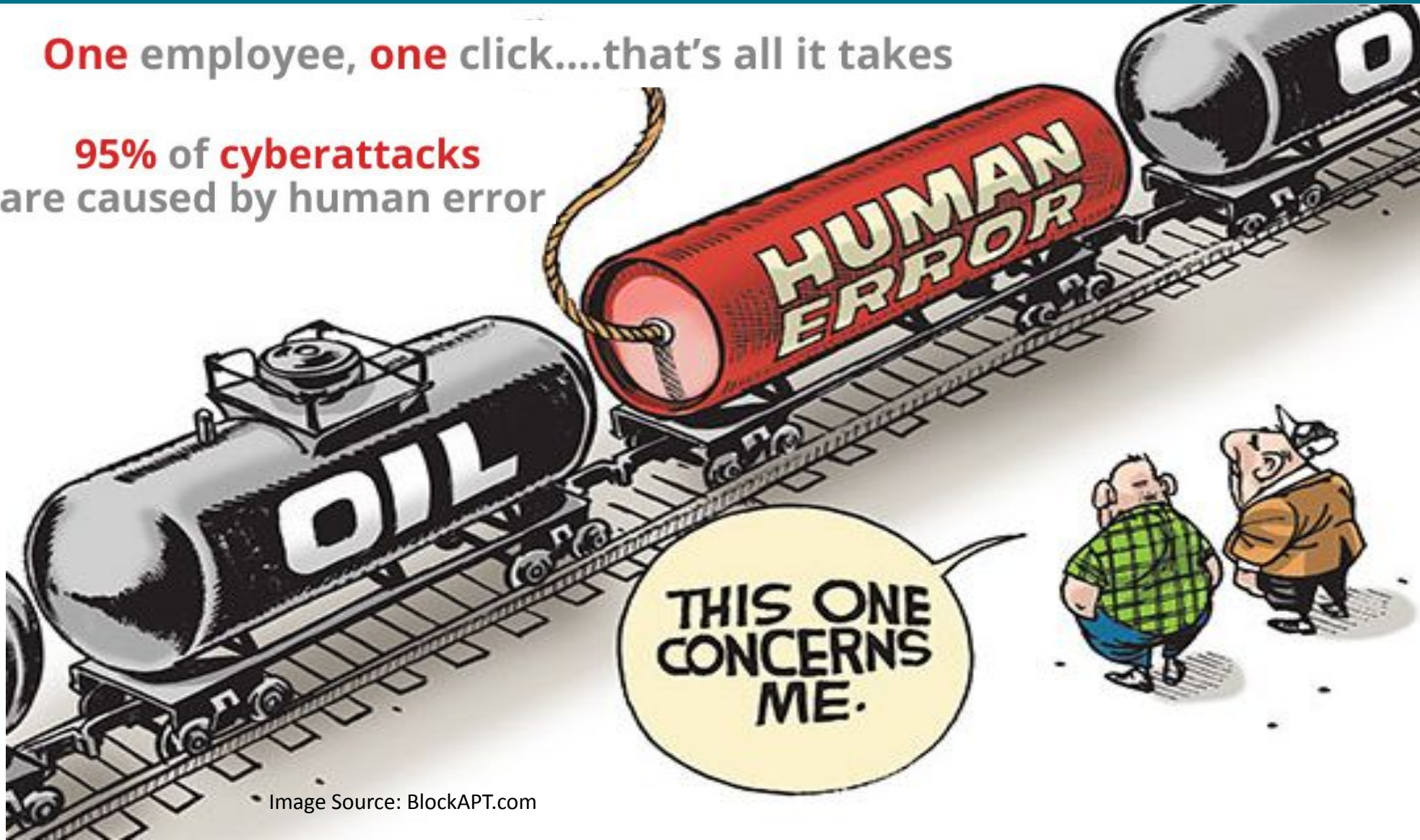


Image Source: BlockAPT.com



CYBER RISK MANAGEMENT



DO YOU HAVE AN IT STRATEGIC PLAN?

Damage or theft of
IT assets cost an
average of
\$1,027,053.

Disruption to
normal operations
cost an average of
\$1,207,965.



Sandberg

“Make the plan ahead of time, print the plan, and have it all over the place,” said Chris Sandberg, vice president of information security at Trimble Transportation. “You should test every so often that the steps you have in place for the business haven’t changed and don’t need to be [updated] — at minimum annually, but preferably quarterly.”

CYBERSECURITY REPORTING TOOLS



- Companies take 192 days, on average, to detect a breach and another 60 days to contain it, according to an IBM report.
- Companies that contain a breach in less than 30 days save more than \$1 million in comparison to those who take longer.

QUESTIONS



CONTACT

Antonina K. McAvoy, CISA
Senior Manager, PBMares, LLP
Cyber & Control Risk Services
Phone: (757) 355-6011
amcavoy@pbmares.com





www.pbmares.com

MARYLAND - Baltimore • Rockville
NORTH CAROLINA - Morehead City • New Bern
VIRGINIA - Fairfax • Fredericksburg • Harrisonburg • Newport News • Norfolk • Richmond
Warrenton • Williamsburg