




ARE YOU
COMPLIANT WITH
YOUR CYBER
INSURANCE
POLICY??

**GRAB
SOMETHING TO
WRITE WITH**





WHY THE HECK DO YOU
CARE WHAT I HAVE TO
SAY?

- **Matt Horning**
- CEO – Blue Tree Technology

- Started doing IT in 1997
- Been running my own IT business since 2001
- Cyber Security Author - "From Exposed to Secure. The Cost Of Cybersecurity And Compliance Inaction And The Best Way To Keep Your Company Safe"





WHO IS BLUE TREE TECHNOLOGY

- Founded in 2019 by the merging 2 long standing IT companies
- Currently have a Staff of 12
- We work with small to medium businesses and small cities
- Core focus is protecting businesses from Cybercrime
- Secure IT · Secure Peace of Mind



**HOW BAD IS
CYBER CRIME?**

All Tech News > category news Security > category news CyberCrime

Ransomware Attack Blamed As Logistics Firm Collapses

Tom Jowitt, September 27, 2023, 3:44 pm



Devastating ransomware attack blamed, as veteran firm KNP Logistics enters administration with 730 jobs lost

NEWSLETTER

Subscribe to our best articles

Your email →



LOGISTICS COMPANY CLOSES

- 730 Jobs Lost

ILLINOIS HOSPITAL CLOSES

An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.



St. Margaret's Health in Spring Valley, Ill. Google Maps

f X Email Link | SAVE [Create your free profile or log in to save this article](#)

June 12, 2023, 10:25 AM CDT

By Kevin Collier

An Illinois hospital will shutter its doors this week in part because of a devastating cyberattack, which experts say makes it the first hospital to publicly link criminal hackers to its closure.


FOX4

Watch FOX4 ▾ Mornings ▾

NEWS

Jackson County IT systems down, ransomware attack won't impact elections

by: [Olivia Johnson](#), [Regan Porter](#)
Posted: Apr 2, 2024 / 11:30 AM CDT
Updated: Apr 3, 2024 / 12:07 AM CDT



▶ 🔊

SHARE



KANSAS CITY, Mo. – Jackson County has reported ‘significant disruptions’ in its IT systems due to a confirmed ransomware attack.

The interference comes just hours before critical elections in the Kansas City area. However, according to Jackson County, the system outage will not impact the Kansas City Board of Elections and Jackson County Board of Elections.

JACKSON COUNTY RANSOMWARE

- Requests money from the State of Missouri to cover the event




LIBERTY HOSPITAL CYBERATTACK VICTIM

Kansas City, MO 64154 83° Sunny 0% Change 1/1



RECOMMENDED


- Father-daughter doctor duo deliver first baby at new Oklahoma women's center
- Chicago shooting kills 8-year-old girl and wounds 10 people including small children, police say
- A Congressman wanted to understand AI. So he went back to a college classroom to learn
- 'Truly inspiring': Woman prepares to fulfill dying wish of running Boston Marathon
- Committee in support of the Royals' plans for new ballpark in the Crossroads names its co-

As Liberty Hospital computer issues continue, cybersecurity expert says hospitals have become prime targets




Share   

KMBC NEWS Updated: 6:47 PM CST Dec 22, 2023
Infinite Scroll Enabled

Andy Alcock  
KMBC 9 News Reporter



DIFFICULT SPOT
LIBERTY HOSPITAL

2:04   

THIS IS A HUGE PROBLEM

Country	GDP
United States	\$25.463 Trillion
China	\$17.963 Trillion
CYBER CRIME	\$13.82 Trillion
Japan	\$4.231 Trillion
Germany	\$4.072 Trillion

- Cybercrime is estimated to cost the world close to \$10.5 trillion a year by 2025
- \$13.82 trillion by 2028
- That would make it the 3rd largest GDP if we were talking nation states
- This is a huge problem that we all need to work on

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and right-angle turns, ending in small circles that represent components or nodes. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

WHAT DOES THIS TELL US?



“**Anyone** can fall victim to cybercrime and any computing device can be infected with malware. **Nobody** is immune to cybercrime”



**WHO IS GETTING HURT BY
CYBER CRIME?**



CASE #1 – THE INCIDENT

- A ransomware attack cripples a manufacturing company of 200 employees
- Encrypted Business Data
- Encrypted Production Systems
- Attack entered their environment through unpatched system

CASE #1 – THE COSTS

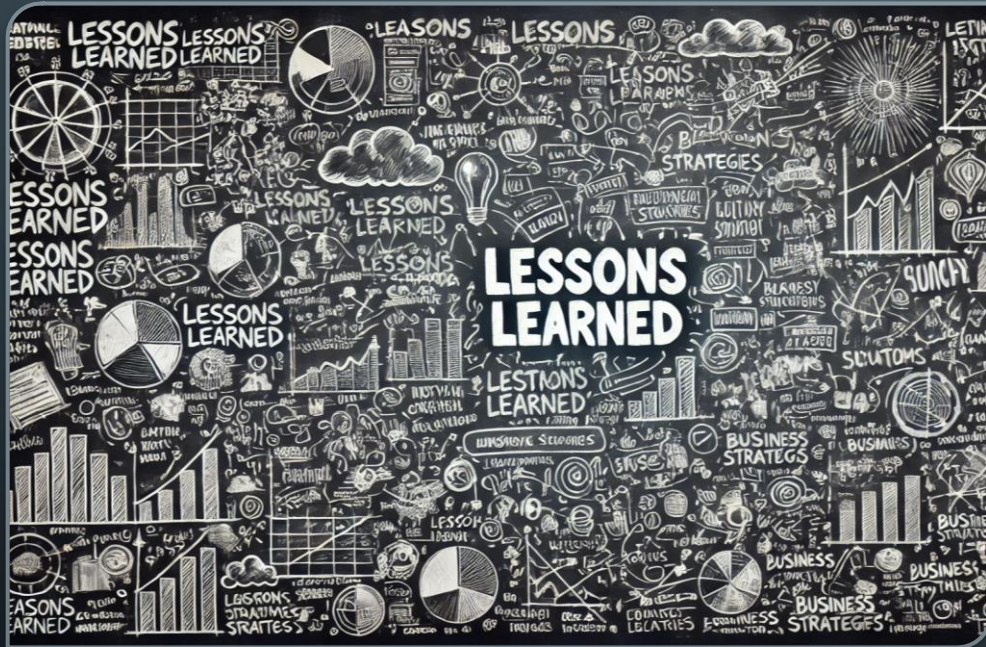
- Ransom Demand = \$500,000
- Ransom Stopped Production for 5 Days = \$750,000
- System Recovery Costs = \$200,000
- Forensics = \$100,000

Total Costs = **\$1.55 Million**



This Photo by Unknown Author is licensed under [CC BY](https://creativecommons.org/licenses/by/4.0/)

CASE #1 – WHAT WAS LEARNED?



Patching is critical

Turn off un-needed
services

Use MFA



**MICROSOFT: 99.9 PERCENT OF HACKED
ACCOUNTS DIDN'T USE MFA**



CASE #2 – THE INCIDENT

- The victim is a real estate firm
- Attackers impersonate a senior executive
- They convince the finance team to wire away \$175,000
- This is called a business email compromise (BEC) scam

CASE #2 – THE COSTS

- Immediate financial loss: \$175,000
- Forensics investigation: \$50,000
- Security improvements: \$75,000
- Legal consulting: \$25,000
- Total claim: **\$325,000**





ACCORDING TO THE FBI'S INTERNET
CRIME COMPLAINT CENTER (IC3), IN
2022, THE AVERAGE LOSS PER BEC
INCIDENT WAS APPROXIMATELY
\$124,000



**CLAIM
DENIED**

CASE #3 – THE INCIDENT

- Illinois manufacturing suffers a ransomware attack
- 2nd one within two years
- Threat actor gained access to desktops and servers

CASE #3 – THE COSTS

- Cyber insurance company (Travelers Insurance) denied the claim
- Found that the company had misrepresented their answers
- MFA was only installed on the firewall and not other digital assets
- Both companies agreed to dismiss the lawsuit and pay their own lawyer fees



CASE #3 – WHAT WAS LEARNED?



- Answer your Cyber Insurance questions accurately
- Use MFA on all possible assets
- Backup critical data



60% OF BUSINESSES THAT SUFFER MASSIVE DATA LOSS
TEND TO SHUT DOWN WITHIN **SIX MONTHS** OF THE
EVENT



WHAT CAN YOU DO?



Cybersecurity doesn't have to be complex or confusing.

Just treat your computer and Cellphone the same way you'd tread your dream car.

Barbie-themed Maserati Grecale Trofeo
\$330,000 530-horsepower

Think in layers

OGRES ARE LIKE ONIONS, ONIONS HAVE
LAYERS, ~~OGRES~~ **CYBERSECURITY** HAVE
LAYERS.





THE HUMAN ELEMENT LAYER

- Start persistent & consistent cyber training with your employees
- Use a password manager – More than 15 characters
- Use technology that scans your Microsoft Office or Google tenant for suspicious activity
- Filter email from SPAM and malicious attachments
- Put Multi Factor Authentication (MFA) on everything you can
- Backup your data



THE NETWORK LAYER

- Nearly half (47.4 percent) of all internet traffic came from bots in 2022
- Install a newer, managed firewall
- Break your network into separate networks. One for your employees, one for any guest access and one for your credit card machines
- Do not allow unmanaged devices on your employee network. This would be phones, Alexa type devices, or game devices like Xbox



EMPLOYEES DEVICE LAYER

- The average time to identify a breach is 207 days
- The likelihood that a cybercrime entity is detected and prosecuted in the U.S. is estimated at around 0.05 percent
- Use Managed Detection Response and Managed Threat Response on all desktops. Yes, Apple too
- Take away local administrator from all employees and the owner
- Uninstall all non-business software from your employee machines
- Use VPN's
- Backup your data



COMPLIANCE LAYER

- 66 percent of companies say that compliance mandates are driving spending
- 78 percent of companies expect annual increases in regulatory compliance requirements
- Do you have Cyber Insurance – Abide by the policy
- Do you take credit cards? – PCI Compliance
- Are you in the medical industry? – HIPPA Compliance
- Do you work with the Department of Defense? – NIST Compliance
- Are you a CPA, Data Broker, Retailer, Financial Advisor, and many more – FTC Safeguards

A close-up photograph of a pen writing on a document. The document has a dotted line and some faint text. A white circuit board overlay is visible on the left side of the image. The background is a dark blue gradient.

CYBER INSURANCE LAYER

- Buy Cyber Insurance
- Your E&O will not cover a cyber event
- Work with your IT team to make sure you are following your policy
- If you are not going to follow the policy, you are self insuring
- Do not keep your policy on your network. Keep a printed version



INCIDENT RESPONSE PLAN LAYER

- More than 77 percent of organizations do not have an incident response plan
- What happens when X happens?
- Who do we call first?
- Who does recovery?
- Make a printed copy and store it at the office and somewhere else safe

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and small circles, resembling electronic components or connections. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

AND ONE MORE THING

THE IMPORTANCE OF CYBERSECURITY FOR GRANDMA

- Teach them the risks
- Invest in Technology that will filter their Internet
- Setup notifications on their bank accounts to you
- Gift Cards are BAD
- Love on them





CONCLUSION: WHAT IS THE PRICE TO PROTECT YOUR BUSINESS?

- The average ransomware payout has increased dramatically from \$812,380 in 2022 to \$1,542,333 in 2023
- The average cost of a ransomware recovery is nearly \$2 million
- Protect your business in layers
- Work with your IT team to make sure your layers are in place
- Compliance is a journey. Work with your IT team for success
- Purchase cyber insurance
- Build and test your incident response plan
- Need someone? Blue Tree Technology is here to help



QUESTIONS?



THANK YOU

- Matt Horning
 - 816-256-2595
 - matt@bluetreetechnology.com
 - QR Code = Discovery Call
 - Free 3rd Party Cyber Security Assessment

Secure IT · Secure Peace of Mind