
The Institute of Internal Auditors

Our Mission

The only time that people hear about hacks or cybersecurity is when the “Black Hats” win. “

Our mission is to support the Community and to say THANK YOU by shining the light on all of the unsung heroes who toil in anonymity to keep us safe while online at work, home and school”. 
Today’s Discussion

1. A View from the C-Suite: An Insider Threat Case Study
2. Meet the “Forrest Gump of Cyber Security”
3. The BIG Pivot: From Victim to Advocate
4. The Future
1. A View from the C-Suite: An Insider Threat Case Study

- 100+ Employees.
- Sold 49% to one of the largest marketing companies in the world.
- AT&T, Best Buy, Ford, General Motors, P&G etc. as clients.
Daily Parking Lot Summits of Trusted Employees

- Near-death injury.
- Small group of employees started their OWN company while working for us full-time.
  - Duplicated website
  - Redirected calls
  - Stole intellectual property
- Called biggest clients alleging fraud.
- Lost Millions.
We lost everything...and so did all of our employees.
Thank you veterans

During the following 10 years, we co-founded The Anthem Project

Co-founded Grasp Learning
Like Phoenix...rising from the ashes.
Spoofed Linkedin 2FA

Gary Berman
Re: Gary, please verify your new device
To: Linkedin Security

On Thu, Mar 22, 2018, 2:07 PM Linkedin Security <security-no reply@linkedin.com> wrote:

Hi Gary,

We noticed you recently tried to sign in to your LinkedIn account from a new device.

You can finish signing in to your LinkedIn account by following the instructions that we sent to your phone number ending in 2632 (US).

If you’re having trouble signing in, please visit the LinkedIn Help Center.

Thanks for using LinkedIn!
The LinkedIn Team

When and where this happened:

Date: March 22, 2018, 2:07 PM
Browser: IE
Operating System: Windows 8.1
Approximate Location: Miami, Florida, United States
Cybersecurity Experts

I could not afford a complete analysis, 90% chance of Man in the Middle Attack

Client Security Report

Gary Berman

Conclusion:
The log files were deleted before 09/15. The laptop was compromised through one of the multiple vulnerabilities with a probability 90%. The list of vulnerability of that OS version includes OpenSSH (the remote access to console) and mitm or network intrusion with privilege escalation. Hacker can gain access remotely with high privileges and destroying all the signs of their deeds. Such as the destroying logs that were before 09/15.
Worked non-stop to gather photographic evidence. 19 Attack Vectors
Apple Genius Bar Work Authorization

"Bluetooth module could not be detected".
Google 2-Step Verification was Spoofed on iPhone

Masked 5 Digit Number

Spoofed 10 Digit Number

Correct Single Use Unique Codes

Same Number Every Time
Multiple attempts to “clean” mobile devices were hacked.
Thunderstrike signature to indicate that hack has begun
Desktop Spoofed

Correct Login

Grey Sand

Clouds and Different Color Sky

No Login
Multiple E-mail Systems Compromised

- Blue vs green color
- No country of origin
- No customer support number
- No logo
- Privacy policy error message
Norton VPN Spoof.
Norton VPN Spoof.

Amazon “The Tick”
Nord VPN Spoof

No Sound
Fiverr Facebook Re-direct

21:48 February 28, 2019

elkararts
It usually Carries an extra charge
02:38 March 01, 2019 | Report

elkararts
And for future adviso, please inform the artist of extra additions before the order starts
02:43 March 01, 2019 | Report

Me
Thank you! I'm learning. I'll make it up to you with a $5.00 tip. Please send the final version. Gary
04:17 March 01, 2019

Me
It's not allowing me to accept delivery. I guess you have to re-send it and I'll accept. Great job!!!
04:31 March 01, 2019

Last seen 1 hour ago | Local time Fri 10:32

Type your message here...

101 / 2500

Facebook
Sim Swapped: SIM was locked and I had to replace it 6 times within one week. Then, it was locked a different way and required a Personal Unlock Key (PUK).
AT&T Hotspot on my cell phone was NOT provisioned by AT&T

Hi, Gary. Today we discussed the mobile hotspot option on the 2632 mobile phone number. I reviewed your rate plan and found that the AT&T Unlimited Choice plan does not include hotspot capabilities. I also reviewed your technical entitlements in our backend system and found that you do NOT have hotspot capabilities or access points provisioned by AT&T. You indicated that the hotspot is working from your device. In my 13 years' experience I have not seen the hotspot work without the correct plan/entitlements.

If you need additional information, please feel free to reach out to AT&T at 1-800-331-0500.

Thanks!

L. Jason Carroll
CS - Team Manager - Advanced Technical Support - Call Center
AT&T Mobility —

AT&T

MOBILIZING YOUR WORLD
Buick confirmation of 36 connected vehicles via On Star.
AT&T Spoofed Bill for more than $9,000
57 Potential Consequences of an Insider Attack as per Carnegie Mellon’s Insider Threat Report

- Physical/Digital
- Economic
- Psychological
- Reputational
- Social/Societal
Law Enforcement

- Local Police Department (5 times).
- FBI (4 times).
- Secret Service (2 times).
- District Attorney declined to open case due to lack of evidence/attribution.

“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”
Justice Louis D. Brandeis
2. Meet the “Forrest Gump” of Cyber Security
“The Heroes Journey” by Joseph Campbell

Endpoint protection
Endpoints are typically the initial target of an attack because they're relatively vulnerable due to the vast diversity of software applications and versions they run, and can thus provide an entry point to the network and access to data that an attacker wants. Legacy endpoint protection, such as host-based antivirus software, has the same weaknesses as other legacy signature-based technology, in that they can only detect malware that is already known—and are completely ineffective for detecting new, modified, or unknown malware threats. Additionally, endpoints such as users' laptops and mobile devices are often not protected by firewalls or IPSs when they're not connected to the organization's network, opening them up to attack when employees use them remotely.
3. The BIG Pivot: From Victim to Advocate.

Joseph Campbell “The Heroes Journey”
THANK YOU Stan Lee: “The Marvel Way”

- Sphere | Cube | Cylinder
- 6 heads high vs 8.5
- Passive vs action
- Average vs heroic
- Bland vs passionate
- Vertical vs forward perspective
The CyberHero Adventures: Defenders of the Digital Universe
Meet the CyberHeroes!

**Meet the CyberHeroes!**

**Queen Jio**

Meet Queen Jio, the reluctant tech lover who became the world’s first female tech hero. She started out as a普通市民, but when a tech villain threatened the city, she joined the team to fight back. Queen Jio is known for her quick thinking and her ability to use technology to outsmart her opponents. She is also the only hero with the ability to hack into any system, which makes her a valuable asset to the team.

**Larry Jones**

Larry Jones is a tech genius who became the world’s first tech hero. He started out as a computer programmer, but when a tech villain threatened the city, he joined the team to fight back. Larry Jones is known for his quick thinking and his ability to use technology to outsmart his opponents. He is also the only hero with the ability to hack into any system, which makes him a valuable asset to the team.

**Tara Bight**

Tara Bight is a tech genius who became the world’s first tech hero. She started out as a computer programmer, but when a tech villain threatened the city, she joined the team to fight back. Tara Bight is known for her quick thinking and her ability to use technology to outsmart her opponents. She is also the only hero with the ability to hack into any system, which makes her a valuable asset to the team.

Copyright Cyberman Security, LLC
Meet the CyberHeroes!

Justina is a first-generation American of Mexican heritage. From a young age, she desired to defend the defenseless. Since then, she realized that she would be a lawyer. She set out to learn all she could about the judicial system. Many times, after she became a Public Defender, defending the rights of the accused, she felt something snatching happened to Justina and her colleagues, when she clicked on an email and all the computers in the office froze.

Justina: Jasco & the Defender

Leonidas served his country with distinction as an officer in the military. He and his family made countless sacrifices in service to America. Unfortunately, during a particularly vicious battle with the Enemy, Leonidas was gravely wounded and confined to a chair for the rest of his life.

Leonidas: The Cybersoldier

Copyright Cyberman Security, LLC
Say “Boo” to the Villains!
Say “Boo” to the Villains!

Sonny the Social Engineer

Ivan the Identity Thief

Randall R.A.T.

Copyright Cyberman Security, LLC
4. The Future

Speeches & Donate Comics to Organizations
4. The Future

16 DHS Critical Infrastructure Sectors

Financial Services: “Defending YOUR Money”

Healthcare: “Defending YOUR Health”
Cyber Security Ecosystem Feedback

21,855 Linkedin senior level connections.
Our Mission

The only time that people hear about hacks or cybersecurity is when the “Black Hats” win. “

Our mission is to support the Community and to say THANK YOU by shining the light on all of the unsung heroes who toil in anonymity to keep us safe while online at work, home and school”.