Once you’re connected, you’re protected. (R)
Who is this guy? Why should we put our phones away?

Mr. Stutzman is a cyber security expert with over 30 years of experience. He oversees information security operations and Virtual Chief Information Security Officers protecting several high net worth families, and small and medium sized companies. He personally serves as the Virtual Chief Information Security Officer for a Manhattan based Private Equity firm, a $3.5bn Oil and Gas, and for the US and LATAM risk operations for a 600,000-employee diversified services company.

Past positions include:

- **Chief Intelligence Officer** – Wapack Labs, Cyber Threat Intelligence
- **DCISE Director** - GS15 at DoD Cyber Crime Center
- **Principal Engineer**, Carnegie Mellon, Software Engineering Institute
- **Chief Information Security Officer**
  Northrop Grumman Electronics
- **Chief, Cyber Threat Intelligence and Analysis**
  Northrop Grumman Corporate
- **Cisco Systems, Sr. Manager Global IT Risk Management**
- **Navy Intelligence Officer, Information Warfare (cyber)**

**Built and ran**

- DoD/DIB Information Sharing and Analysis Environment
- Northrop Grumman’s anti-cyber espionage team (to chase Chinese spies out of Northrop Grumman’s Global Networks).
  
  - Awarded Presidents Award for IT Innovation, 2008
  
  - Information Security Program of the year.

- **Built and ran**
  

- **Founding member**: Honeynet Project (the home to many of today’s current security tools.)

Certified Information System Security Professional (2002 – Pres), BS Excelsior College, MBA Worcester Polytechnic Institute, Senior Executive Fellow, Harvard Kennedy School

[Mr. Stutzman's Photo]

[LinkedIn Profile](https://www.linkedin.com/in/jefferystutzman/)
Who is Trusted Internet?

- Cyber Security Monitoring Company
- Think “ADT” for your computers
4 days

Why is this important? You’ll see.
18 months ago a company’s IT personnel noticed an ‘anomaly’ in datacenters in the Middle East and Asia.

Two hours later, over 1000 servers had been encrypted, crippling the company and its ability to communicate.

Dead in the water…
Backup systems and data were encrypted.

Had no communications;

Had no idea of the true extent of the damage.

They were losing approximately $25 mil per day.

They were facing an extinction event and had run out of hope.
This is what a $100,000 Bitcoin transaction looks like.
Day 1
First Detection
IT Team unable to contain

Day 2
Extent of damage and scope of attack still unknown

Day 3

Day 4
Trusted Internet engaged
- Board notified.
- FBI Notified.
- Ransom paid.

10:00 PM EST – Decryptor received; first tests performed successfully

Day 5
Priority of Restoration

Day 6
Decryption and restoration of services in full swing.

Day 7
Decryptor operations validated

June – October - recovery

- Polymorphic
- Reboots halted computers
- Spread through backup system
Here’s how it all started: They came through the front door…

- An authorized user mistakenly believed a “software update” was legitimate
- Visited a compromised website, and was subsequently infected with the malware.
- The infection spread through the backup system.
Malware: Dridex, Bitpaymer and PowerShell Empire

- **Dridex** – Steal credentials.
  - Installed by botnet
  - Steals credentials

- **Bitpaymer** - Ramsomware
  - Inserted using stolen credentials
  - Encrypts systems

- **PowerShell Empire** – Uses Windows tools to move around
  - Post exploitation framework used to run modules
  - Used to download Bitpaymer
Two hours later, the company was crippled, operations halted worldwide.
Immediate Actions to Enhance & Harden IT Protections – First 24 hours after decrypt

- Deployed endpoint protection to all endpoints
- Global Password Reset on all privileged accounts
- Imposed restrictions
  - Social media, Cloud storage applications, etc.
  - USB devices
Immediate Actions to Enhance & Harden IT Protections

- Baseline hardening completed
- Retained third party security operations center to monitor global network
- Added over 25,000 pieces of intelligence to current defenses
- Implemented additional advanced security tools to further harden the environment
- Penetration tested
Lessons Learned

- Seconds count
- This can happen to anyone
- Be ready
- These won’t be stopped, but can be managed
4 days

Why is this important?

- Four days was the amount of time that the IT team tried to fix it on their own.
  - before the CEO told the board
  - before the CEO even KNEW that his systems were being held for ransom.
- At a cost of approximately $25 mil per day in losses, $700K in bitcoin, $4 mil in remediation
Things to consider...
Fast Internet is CHEAP.
The instructions don’t mention firewalls (or any security for that matter)
Artificial intelligence (AI) continues to be a focal point for airline investment. AI has become the most common technology that airlines are currently investing in: 44% have a major program (up from 32%) and a further 45% are running a pilot. (SOURCE: SITA)
Targets?
Things you may not have considered…

- Mobiles
- Executives
- The unsuspecting

Cloud and SaaS
Physical Security Systems
Everything leaks
No matter how good you are, or how hard you try…
This is what good networking should look like. (It’s not as hard as it looks)

- Common sense architecture
- Easily implemented, easily monitored.
- Low cost high payoff security infrastructure.
- Gets you compliant quickly with many of your government technical compliance requirements.

Here’s what we use:
- Sophos or FortiNet Anti-virus
- Cisco Meraki Firewall (homes, execs, small business)
- FortiGate Firewall (business)
THANK YOU

Jeff Stutzman, CISSP
Founder & Chief Information Security Officer