

HELION

**Navigating the Aftermath:
Strategies to Mitigate Future
Disasters Post-CDK**




 **Erik Nachbahr**
CISSP #728261

July 2024

www.heliontechnologies.com

HELION

A Dealer asks.....



Do you feel we have in place what we need to limit the 'damage' of an event? Class action, Litigation, FTC... That's some scary s**t. Does anything stand out that we don't have or don't do?

www.heliontechnologies.com

Scary right?



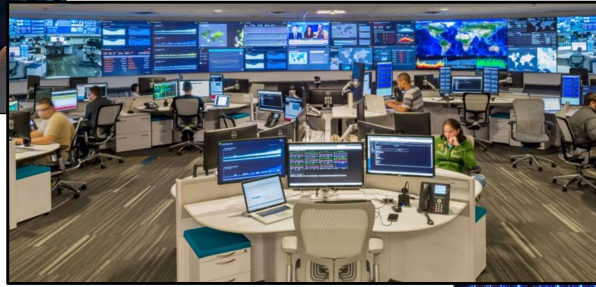
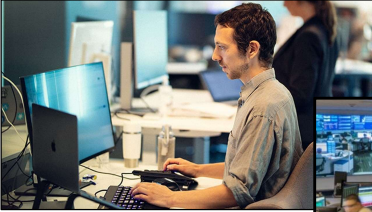
www.heliontechnologies.com

Reality: Unlimited Manpower



www.heliontechnologies.com

Reality: Unlimited Technology



www.heliontechnologies.com

Cybercrime is rising



\$10 Trillion – 2024

\$24 Trillion – 2028

www.heliontechnologies.com

2024 1st Half Major Cyberattacks

HELION

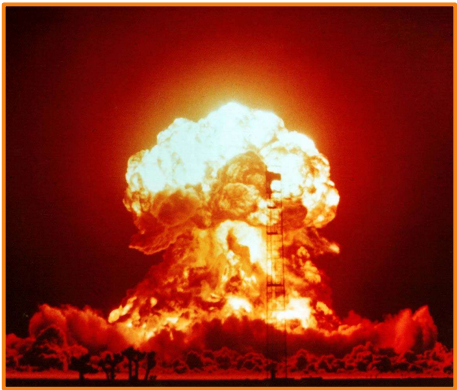
CDK	United Healthcare Frontier Airlines
Findley Auto Group	ThyssenKrupp Fujitsu
My mom	Prudential Financial

www.heliontechnologies.com

Some Consequences

HELION

- Downtime / Lost Revenue
- Reputation
- Attack Mitigation
- Clean Up Cost
- Regulatory Accountability



www.heliontechnologies.com

Opportunity



Reduce Attack Surface



www.heliontechnologies.com

01010101010 010 0 01010 0101010101010101
1010 1010101 101010101 10101010 0101 1 10
10 010 10101010101010101010101 1 10101 101
0 1 0101 01010101010101010 0101010 01011
1010101010101010101 101 1 1010101 10 0101 10
101010101 101010101 101010 10101010101010
101 1010101010101010101 10101010 010101 101
1 10101010101010 01010 000010101010 0101
01000101 1010101 0100100 0 1 1001010101 10
010 0 0101010 1 1010001 00010 010001010101
0 0 101 0 101 101 1 1010 010101010010 0101
1 0101010101 1 10001 0 0 10101 10 1 101
0 1 1 1 1 10 0 0 11 1 01 1 10 11 1

Do we have what we need?

I'm a car guy, not a computer guy



www.heliontechnologies.com

But I Completed the Checklist!



- Online compliance products
- Only as good as the assessor
- False sense of security
- Show your checklist to the hackers!

www.heliontechnologies.com

THERE IS NO QUICK FIX

Do you know your technology?

- IT Team Responsibilities
- Processes in place
- Technologies in use
- Opportunities for enhancement
- Trust but verify



HELION

www.heliontechnologies.com

Essential Security Practice



Annual security review presented in writing to the board of directors.

Performed by a certified individual who examines your business.

www.heliontechnologies.com

Realtime Attacker Hunting



- Security Operations Center (SOC)
- System Log Analytics
- AI Attack Correlation

www.heliontechnologies.com

Account Security

HELION

- Audit Administrator access
- Limit PC admin access
- Secure passwords
- Apply privileges sparingly
- Multi-Factor authentication
- Federated single sign on



www.heliontechnologies.com

Keep Technology Current

HELION

- 4 years before the iPhone
- Beyonce's first solo album
- Michael Jordan's last NBA game
- Arnold Schwarzenegger elected governor
- Oct 2025 Windows 10 Retires



www.heliontechnologies.com

Employee Training



- Security practices go beyond IT
- When hired
- Minimum annually
- Minimum quarterly phish tests

www.heliontechnologies.com

Pen Tests and Vulnerability Scans



- Pen Test: system security tests by human assessors (annual)
- Vulnerability Scan: semi-annual scan and patching of computer systems
- Useless without human, expert intervention



www.heliontechnologies.com

Insurance Coverage

HELION



- Application representations that state “all”
- MFA and administrator representations
- Breach Coach
- Coverage specific to cyberattack

www.heliontechnologies.com

HELION

Erik Nachbahr

✉ Enachbahr@heliontechnologies.com

☎ 443.610.7640

✉ For Slides: Marketing@heliontechnologies.com

🌐 For A Free IT Assessment Please Visit:
www.HelionTechnologies.com/it-assessment



www.heliontechnologies.com