IRONTECH SECURITY

Five Steps to Protect Your Firm from Catastrophic Cyber Attacks

www.irontechsecurity.com

Tom Kirkham, Founder & CEO

IRONTECH SECURITY

RPC Ethics and Confidentiality

ABA *RPC* 1.1, Competency - comment [8]:
"… (ii) keep abreast of… the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

ABA *RPC, Confidentially of Information* - 1.6:
"(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

IRONTECH SECURITY

Common Myths

(Sometimes Heard from 30+ Year IT Pros!)

- “You are Too Small - Who Would Want to Attack You?”
- “You Can’t Afford Enterprise-grade Security”
- “Antivirus is Good Enough and That’s All There Is”
- “You Have Cybersecurity Insurance Anyway”
- “You Survived a Ransomware Attack, So You’re Fine”
- “Cybersecurity Is an IT Issue”

IRONTECH SECURITY

InfoTech versus InfoSec

IT Objectives
(MSP/CIO)

- Productivity
- Efficiency
- Minimize Interruptions
- Bottom-Line Focused

Operations Role

InfoSec Objectives
(MSSP/CISO)

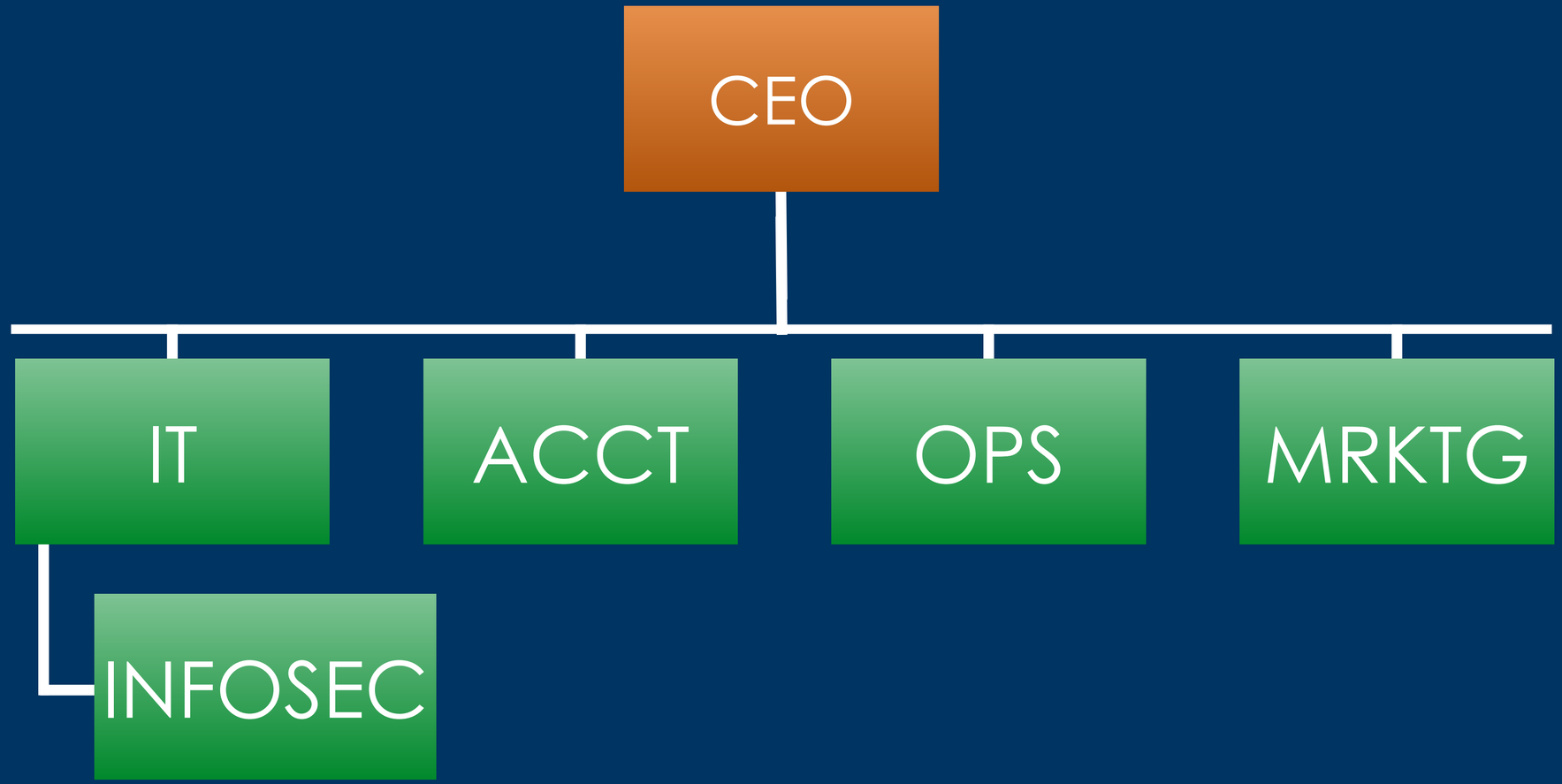
- Understand Risks
- Monitor/Respond Quickly
- Geopolitical Factors
- Protect ALL Stakeholders

Strategic Role

Learn more about MSP versus MSSP: mssp.irontechsecurity.com

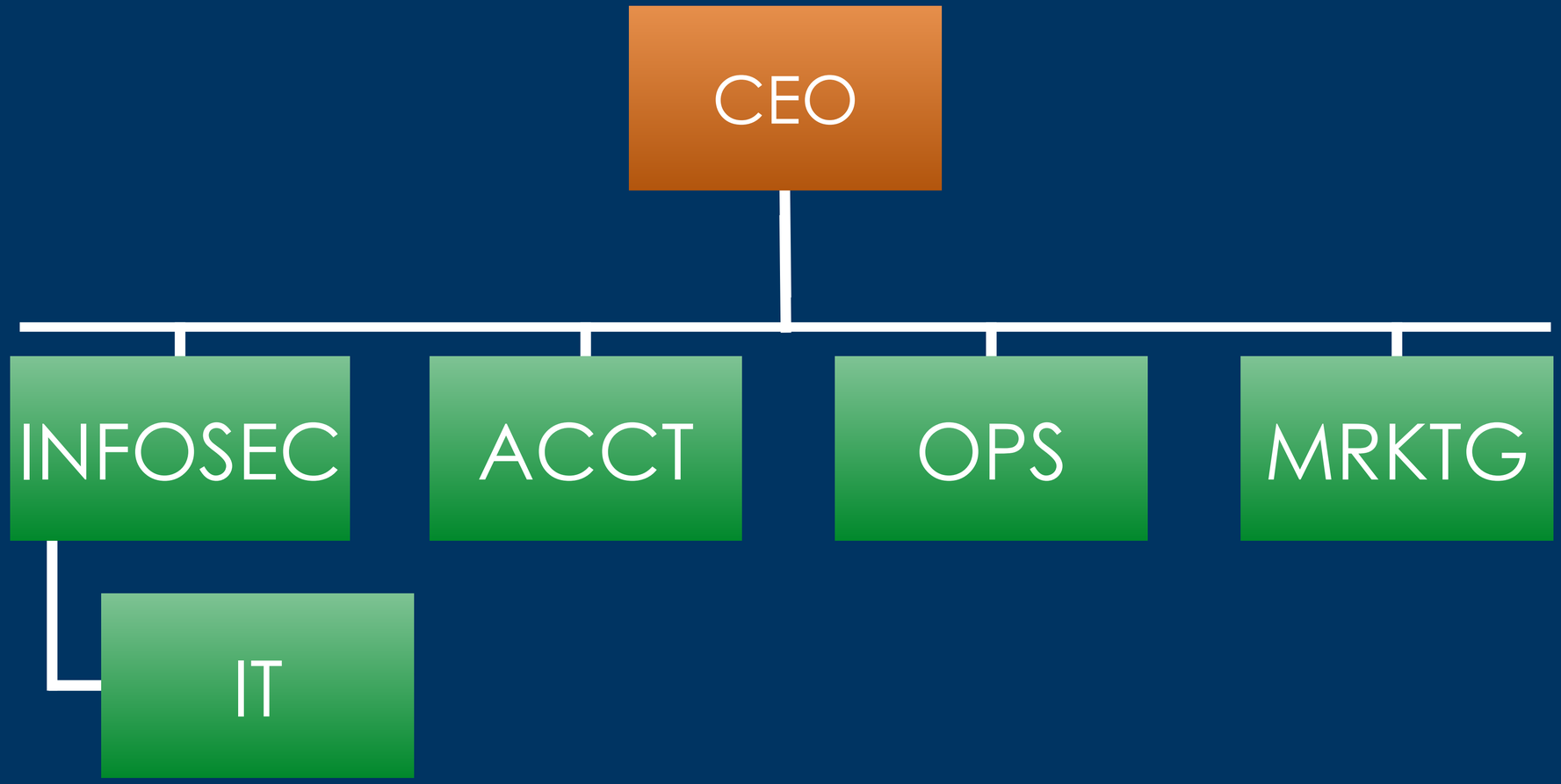
IRONTECH SECURITY

Old Org Chart



IRONTECH SECURITY

Future Org Chart



IRONTECH SECURITY

Cybersecurity Insurance Issues

- Reports of 20-49% of Claims being Denied
- Recent Reports of 200-300% Premium Increases
- Underwriters Requiring Enterprise-level Cybersecurity Defense
- Risk Scoring and Setting Higher Premiums

IRONTECH SECURITY

NIST Cybersecurity Framework

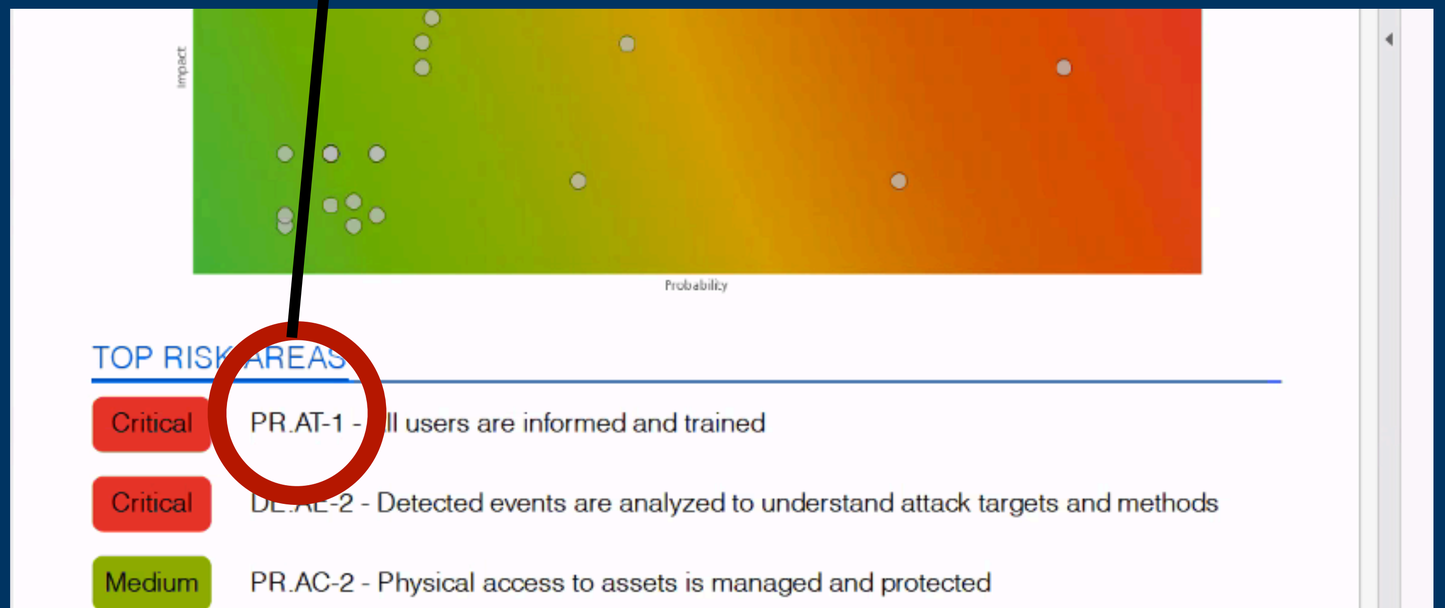


IRONTECH SECURITY

NIST CSF

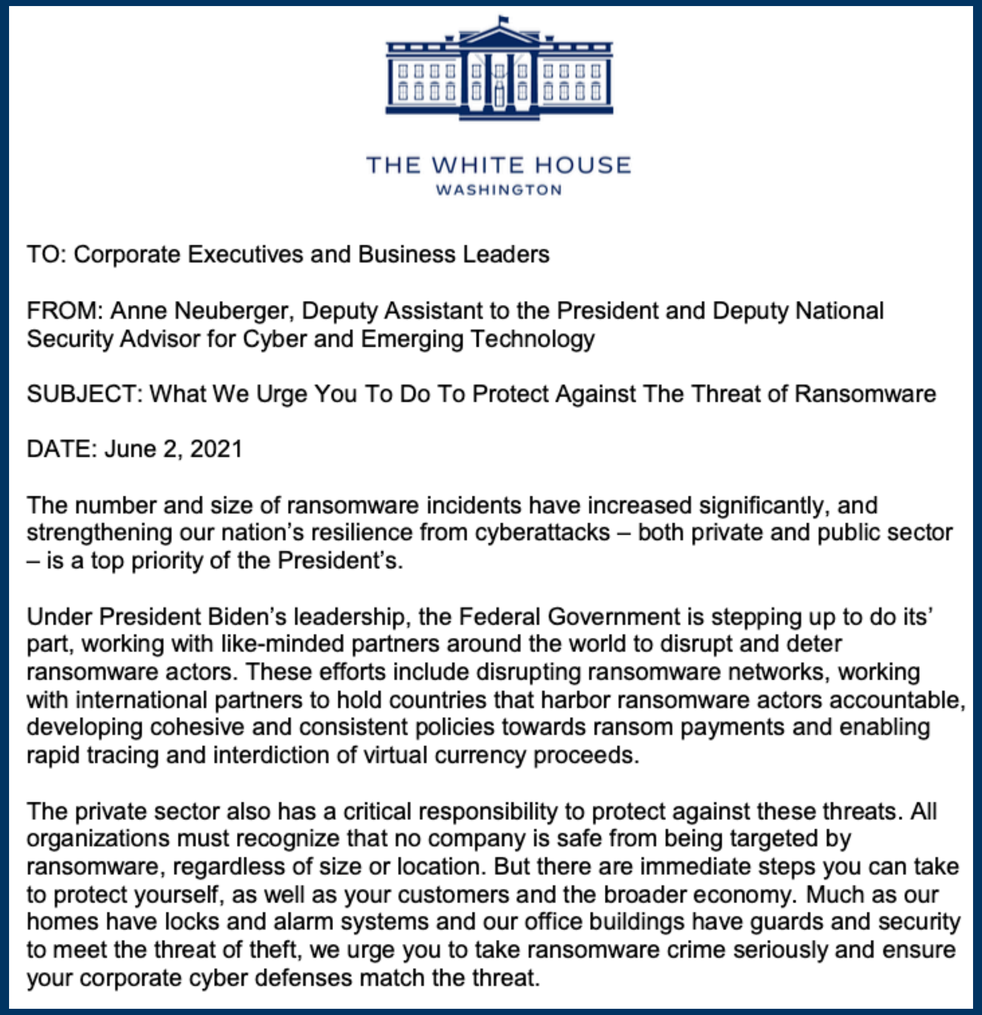
Category	Subcategory	Informative References
		ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies	**PR.AT-1:** All users are informed and trained	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
	PR.AT-2: Privileged users understand their	**CIS CSC** 5, 17, 18

NIST CSF Assessment



IRONTECH SECURITY

White House Deputy National Security Office Open Letter



THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.

5 Best Practices:

- Deploy EDR
- Use MFA
- Storage Encryption
- Continuously Incorporate New Threat Info into defenses
- A Skilled Security Team

IRONTECH SECURITY

Deploy EDR



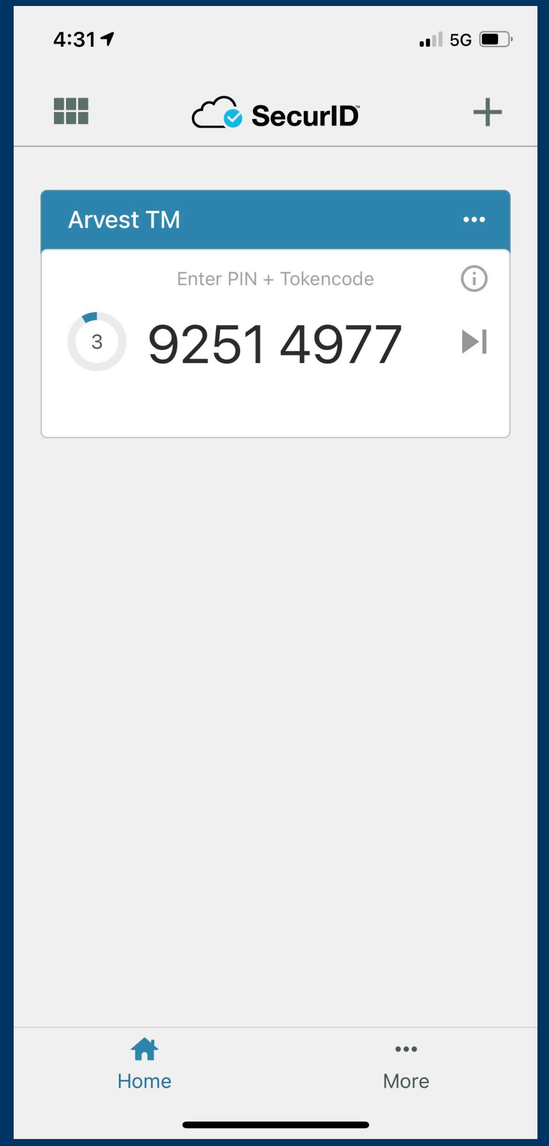
- Endpoint Detect & Respond
- Uses AI and/or ML
- Does not Rely on Virus Signatures
- Also Called MeDR, MDR, XDR, EPP, et al.

Neuberger, WH: “To hunt for malicious activity on a network and block it”

IRONTECH SECURITY

Use MFA

- Multi-Factor Authentication
- Required for Remote Access
- Everywhere that Offers It



Neuberger, WH: "Because passwords alone are routinely compromised"

IRONTECH SECURITY

Use Encryption

- Turn on Disk Encryption
- Required for Portable Devices
- Decrease Attack Vectors



Neuberger, WH: “so if data is stolen, it is unusable”

IRONTECH SECURITY

Continuous Defense Improvements

- Monitor Threat Intelligence
- Adjust Defense as Needed
- Risk-based Assessment of Software Updates



CISA, FBI, Dark Reading, Krebs on Security, IronTech

SIGN UP HERE: threats.irontechsecurity.com

IRONTECH SECURITY

A Skilled Security Team

- 24/7 Monitoring, Investigating, & Responding - Orchestration
- Geopolitical Dynamics
- New Threat Technologies
- New Threat Actors



NO LONGER DIY

Nueberger, WH: “To patch rapidly, and share and incorporate threat info into defenses”

Sign up for Threat Intel: threats.irontechsecurity.com

IRONTECH SECURITY

Other Recommendations

- Company-Owned Equipment to Remote Access
- Password Manager w/Complex, Random Passwords
- Managed & Secure Website
- Secure Encrypted Email

Sign up for Threat Intel: threats.irontechsecurity.com

IRONTECH SECURITY

WH Summary

“…we cannot fight the threat posed by ransomware alone.”

“The private sector has a distinct and key responsibility.”

Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, June 2, 2021

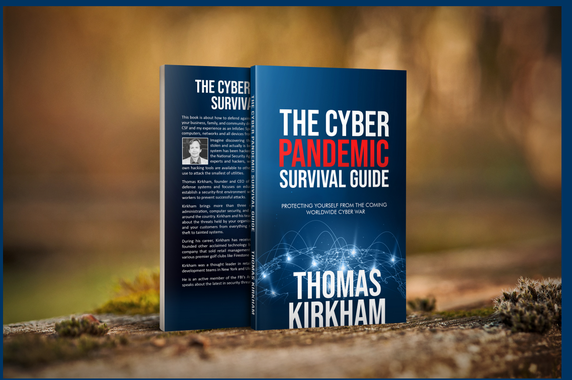
IRONTECH SECURITY

GET STARTED NOW

meeting.irontechsecurity.com

479-434-1400

sales@irontechsecurity.com



Book Notification: www.tomkirkham.com

IRONTECH SECURITY