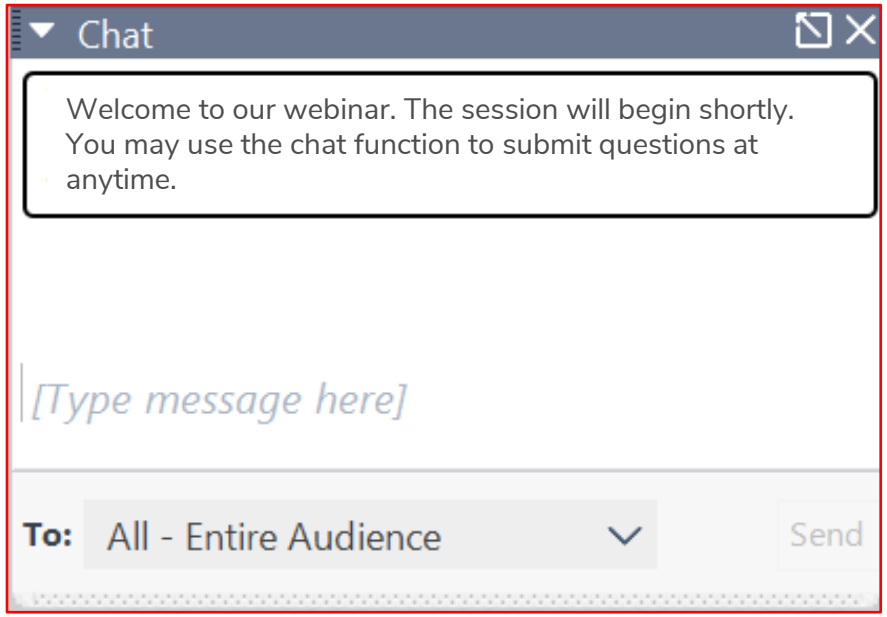
KROLL

10 Essential Cyber Security Controls for Increased Resilience

(and better cyber insurance coverage)

Notes

- Session is being recorded, You'll receive access to the recording in a couple days
- Ask questions via chat >
- We'll try to answer as many questions as possible



Meet The Team

Mari DeGrazia
Associate Managing Director,
Cyber Risk
Kroll

Peter McKeever
Assistant VP, US & Canada Cyber
Practice
Marsh

Jeff Macko
Associate Managing Director,
Cyber Risk
Kroll

Elizabeth Dill
Partner
Mullen Coughlin

Table of Contents

The 10 Essential Controls

Multifactor Authentication (MFA)

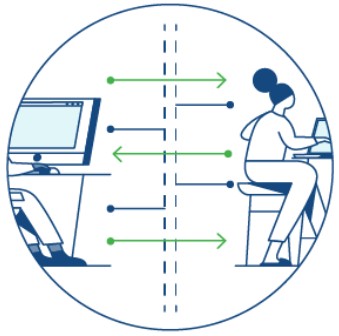
Virtual Private Network (VPN)

Remote Desktop Protocol (RDP)

Endpoint Detection and Response (EDR)

Incident Response Planning

Infrastructure and Segmentation



Backups

Access Control

Security Culture Training

Email Hygiene

Poll #1

Why These 10 Controls?

40+

Cyber insurance application questionnaires and ransomware supplementals

2700+

Incidents handled in 2020, trending upwards of 3000 in 2021

350+

Offensive security engagements

Multifactor Authentication

- Additional forms of authentication increases security
- All users **(including admins)** adhere to MFA procedures
- Should be enabled for every system account
- Ensure audit of implementation

Virtual Private Network (VPN)

- Increased during the pandemic, but requires increased security
- Exploited by adversaries fueled by host of vulnerabilities

BEST PRACTICES:

- PATCH!
- Ensure frequent reviews of VPN logs
- All users should log in with minimum access privileges

Remote Desktop Protocol (RDP)

- Full control of a remote computer, including local network access and storage
- Can be exploited by actors if accessible to the internet without 2FA or MFA enabled

BEST PRACTICES

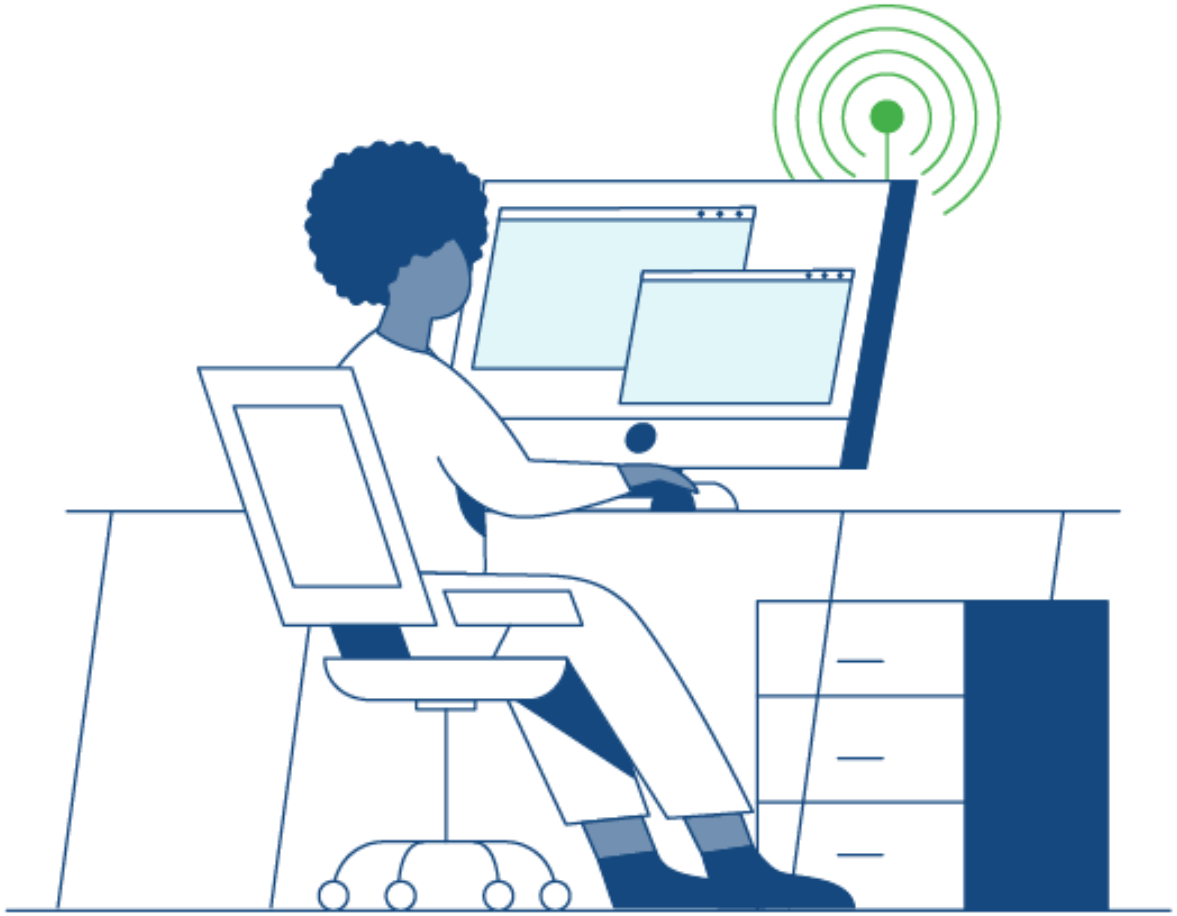
- PATCH!
- Make accessible only via VPN or virtual desktop solution
- Should only be accessible to the internet if 2FA or MFA are enabled

Endpoint Detection and Response (EDR)

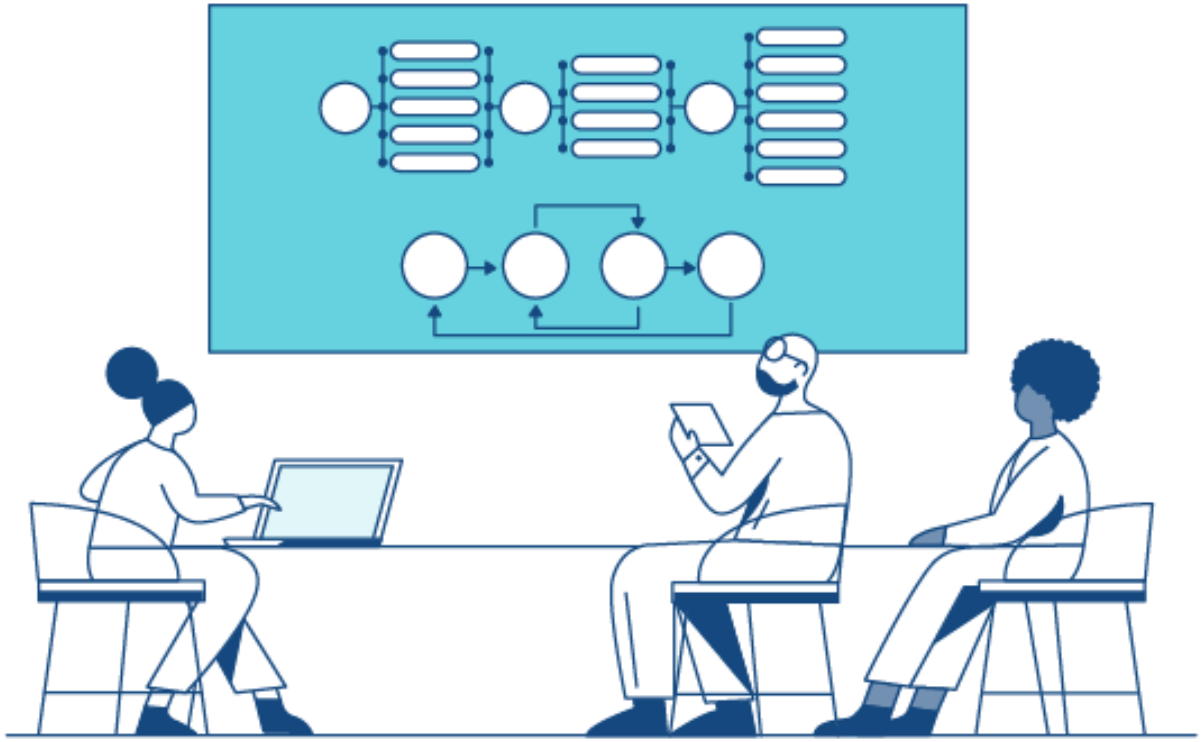
- Lightweight agent deployed on endpoints (laptops, servers, workstations) providing visibility for suspicious behavior
- Looks for network scanning, lateral network movement, and more

BEST PRACTICES

- Should be deployed as wide as possible in an environment
- Team to monitor and validate alerts



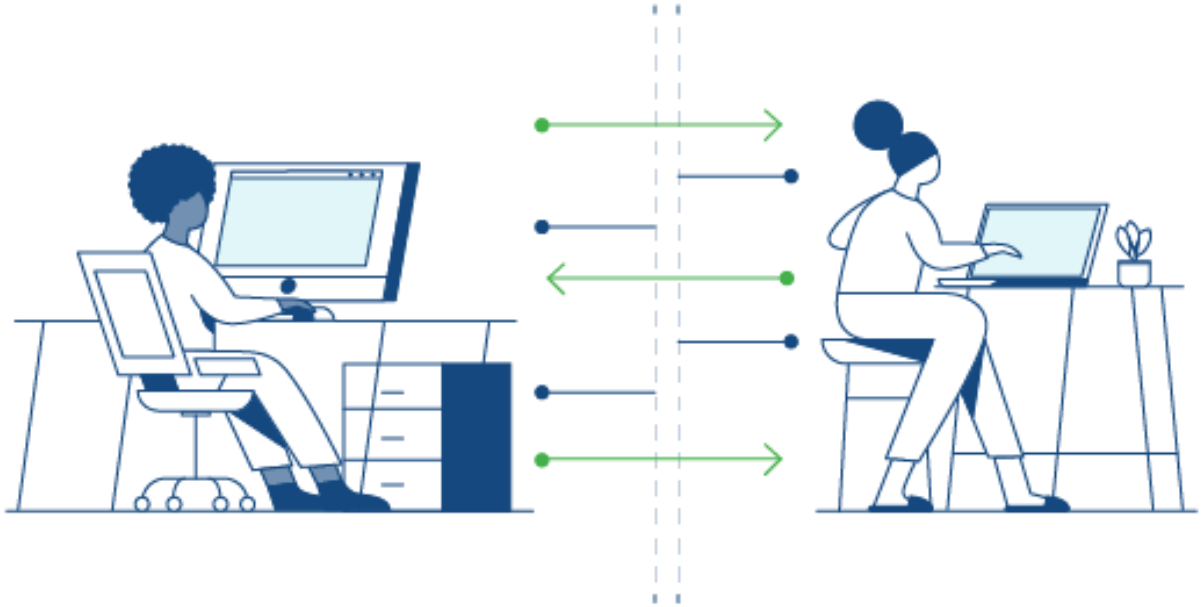
Incident Response Planning



- Should always be accessible in case of incident
- All key stakeholders are identified
- Test and update plan regularly
- Use time wisely – know who to contact

Infrastructure and Segmentation

- Layered approach to security
- Patch management for perimeter devices and 3rd party contracts
- Separate and distinct IT and cybersecurity roles



Poll #2

Backups

- Assess and test recovery capabilities yearly
- Have offline backups – critical with ransomware
- Multiple backups – helpful for data corruption, data loss and malicious events
- Review all data to determine what should be backed up, how often and the best medium

Access Control

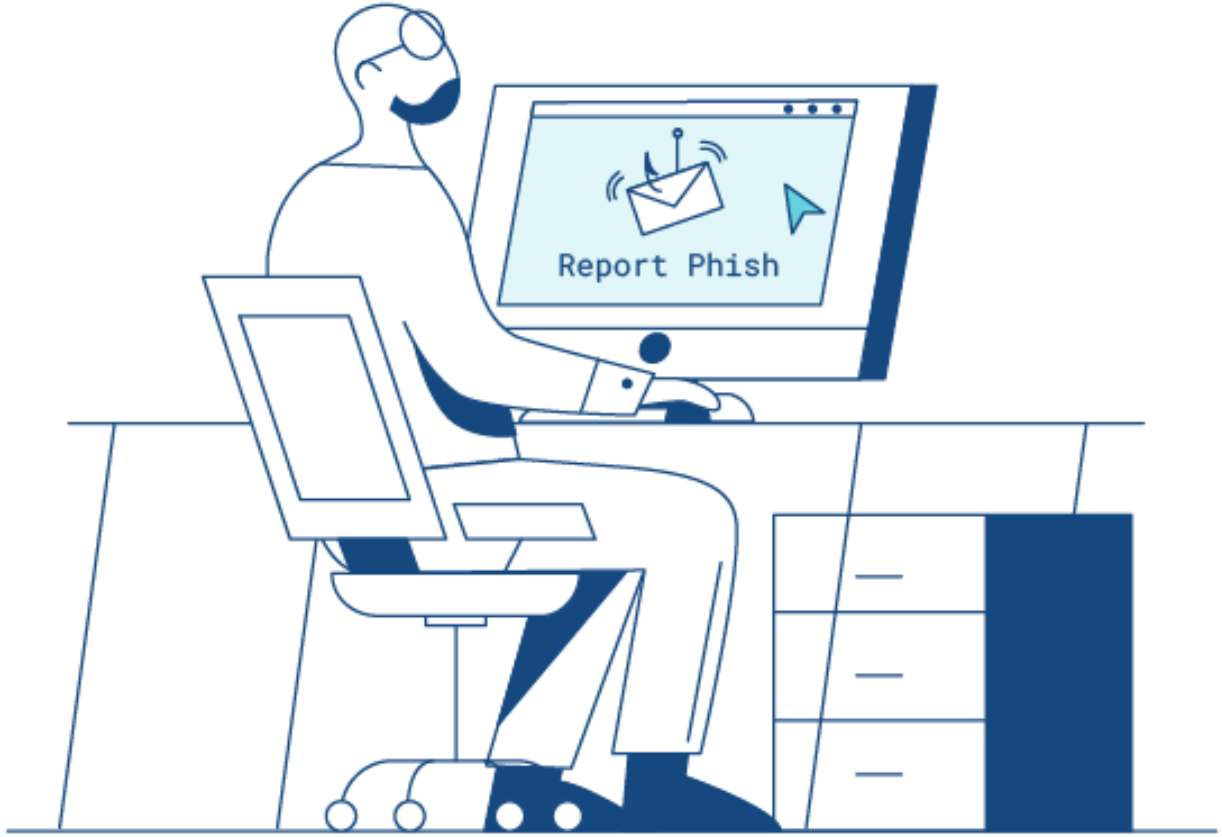
- Institute “least privilege” policy
- Quickly remove access permissions for departed users and adjust permissions when employees transfer roles
- **Regarding IT admins:**
  - privileged-access management solutions
  - Network segmentation
  - Password management
  - Limit admin-level access users

Security Culture

- Empower employees to feel they can raise security concerns and report suspicious issues
- Mandatory cybersecurity training for all staff
- Understand when to retain and delete data
- Provide tools and training for recognizing external email and for validating financial requests

Email Hygiene

- Train employees to identify and report phishing emails
- BYOD – create additional written policies and tech controls to manage associated risks
- Multi-layered defense:
  - Filtering controls on inbound and outbound messages
  - Attachment sandboxing
  - URL rewrites



Q&A

KROLL

For more information, please contact:

Mari.degrazia@kroll.com

Jeff.macko@kroll.com

edill@mullen.law

Peter.mckeever@marsh.com

MULLEN COUGHLIN

Marsh

About Kroll

Kroll is the world's premier provider of services and digital products related to valuation, governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.