Your Ransomware Task Force: Response, Recovery, and Remediation Tips from the Pros

Bill Hardin
Vice-President
Charles River Associates

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

KnowBe4
Human error. Conquered.

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

About Roger

- 30 years plus in computer security

- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security

- Consultant to world's largest companies and militaries for decades

- Previous worked for Foundstone, McAfee, Microsoft

- Written 11 books and over 1,000 magazine articles

- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019

- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)
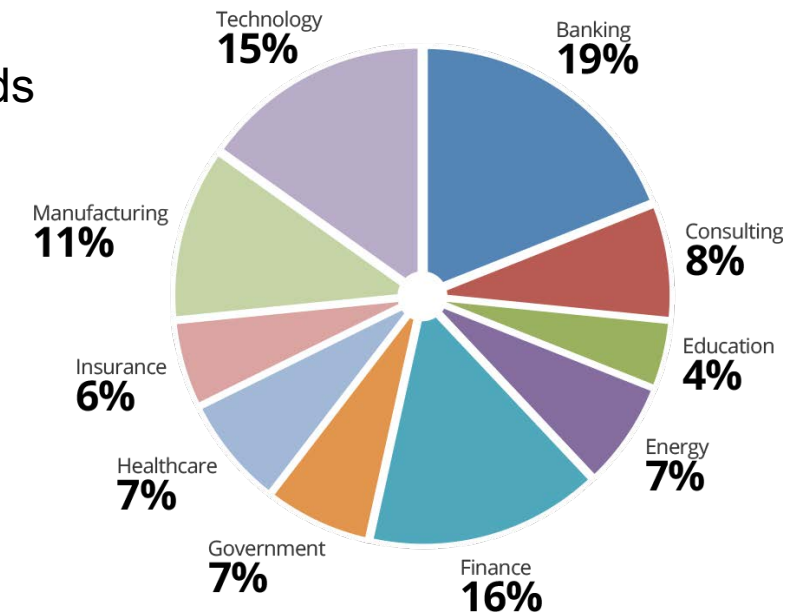
Certification exams passed include:

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform

- Based in Tampa Bay, Florida, founded in 2010

- CEO & employees are ex-antivirus, IT Security pros

- 200% growth year over year

- We help tens of thousands of organizations manage the problem of social engineering

Technology
15%

Banking
19%

Consulting
8%

Education
4%

Energy
7%

Finance
16%

Government
7%

Healthcare
7%

Insurance
6%

Manufacturing
11%

About Bill

Bill Hardin

Vice-President

Charles River Associates

BHardin@crai.com

312-619-3309

- Has worked on thousands of forensic engagements in the areas of data breach and cyber incident response, theft of trade secrets, white collar crime, FCPA investigations, and enterprise risk management.

- Many of his cases have been mentioned in The Wall Street Journal, Financial Times, Forbes, and Krebs on Security, amongst other publications.

- He has spoken at numerous events on cybercrime, risk management, and strategy/operations consulting.

Charles River Associates

- Leading global consulting firm that offers economic, financial, and strategic expertise to major law firms, corporations, accounting firms, and governments around the world.
- In business over 50 years
- www.crai.com
- +1-617-425-3000

CRA Cyber Security Services

Having responded to thousands of clients matters in the cyber security space, Charles River Associates ("CRA") deploys a team of experienced operators to tackle disruption to help our clients get back to business as usual. Our team has an expansive set of skills and capabilities to assist our clients as they respond to and recover from a broad spectrum of cybersecurity matters.

Incident response and investigations

Strategic cyber services

Post-incident review

Our goal is to manage the disruptions and get organizations back to business as usual.

10%   **30%**   **60%**   **100%**

Charles River Associates
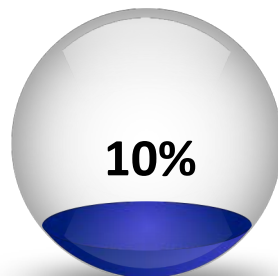
Agenda

Two-Part Webinar

Today - May 20th

- Interview with Bill Hardin
- Cover technical response, recovery, negotiations with ransomware gang

On-Demand

- Interview with John Mullen
- Cover how to handle the first day of incidence response
- What to do and what not to do

EMBER is Burning

1. Extortion
2. Malware
3. Business Email Compromise
4. Engineering
5. Regulatory

CRA Charles River Associates

EXTORTION - RANSOMWARE

RYUK **BitPaymer** vCrypt **Locky**

Stampado Zelta **Lockout** **SAMSAM** **Matrix**

Black Mamba **Dharma** **Cry9** **Serpent** **Jigaw**

Sodinokibi **Clop**

JeepersCrypt CryptoMix **Petya**

Erebus **WANNACRY** **NotPetya Bad Rabbit**

Reveton **Mole66** **Dopplepaymer**

GlobeImposter2 **Netwalker** **Maze**
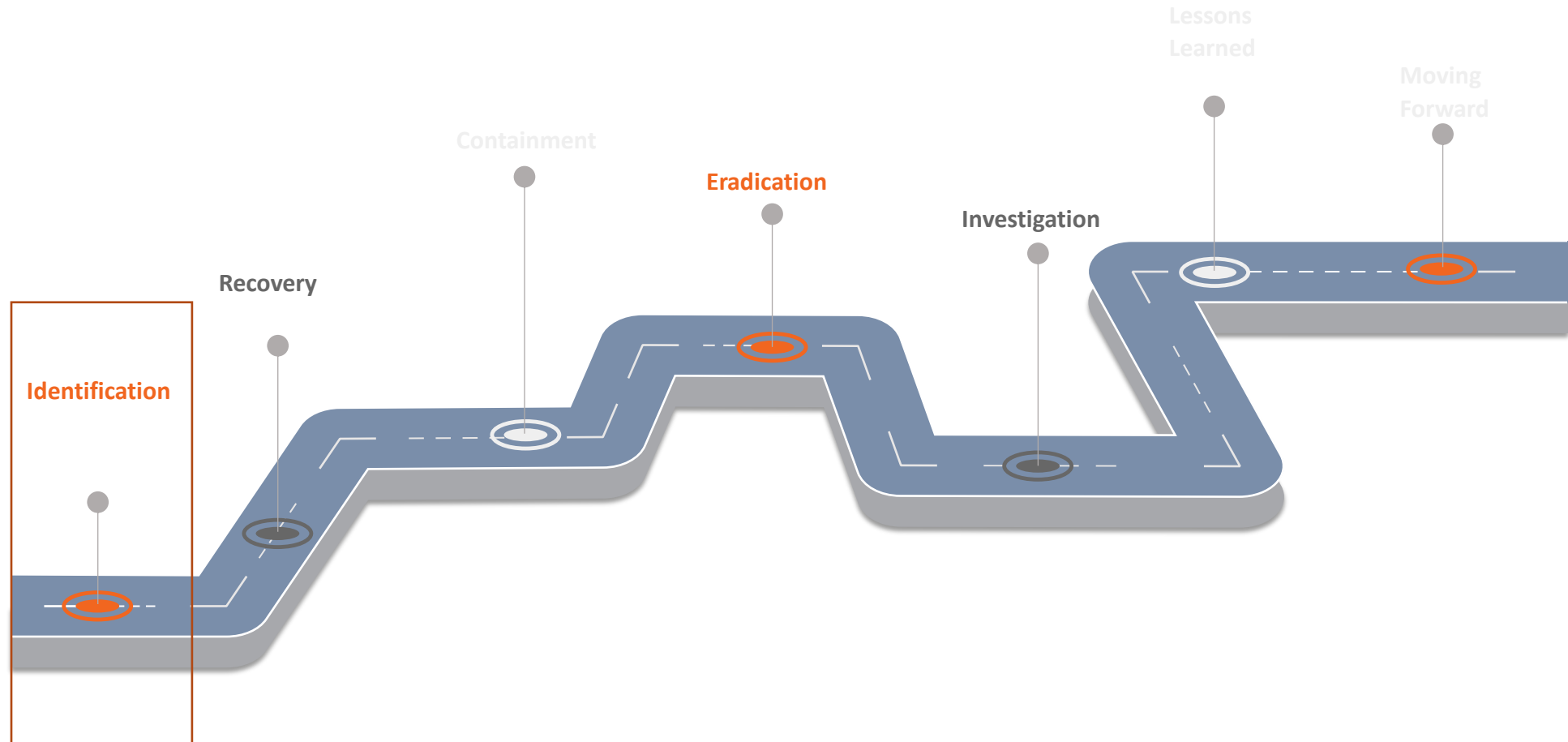
Customers Are Building a Modern Security Stack….

People

Devices

Infrastructure

Network

…That Starts With the Human

KnowBe4
Human error. Conquered.

The KnowBe4 Security Awareness Program **WORKS**

Baseline Testing
Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

KnowBe4
Human error. Conquered.

Security Awareness Training Program That Works

- Drawn from a data set of **over six million users**

- Across **nearly 11K organizations**

- Segmented **by industry type** and **organization size**

- **241,762** Phishing Security Tests (PSTs)
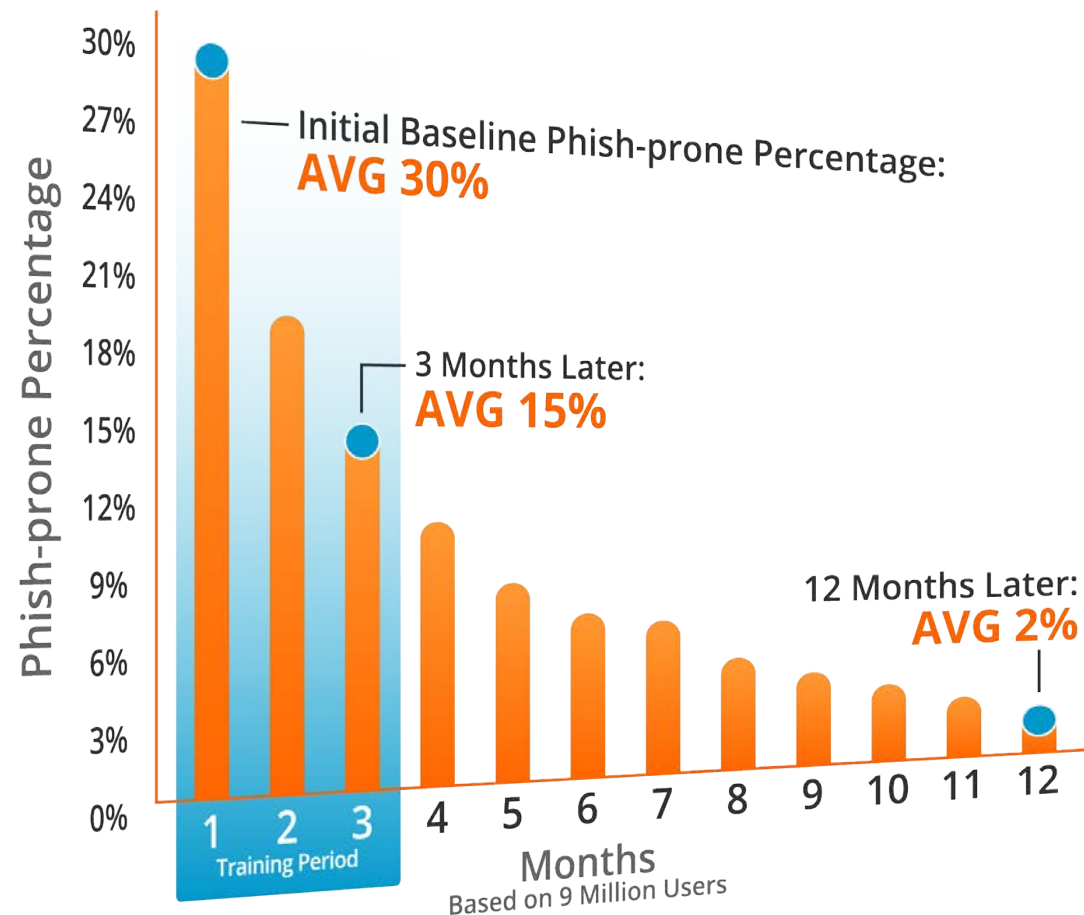
Resources

Free IT Security Tools

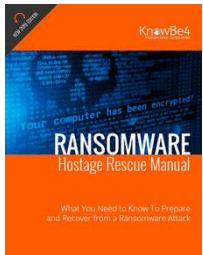|					
Domain Doppelgänger	Awareness Program Builder	Domain Spoof Tool	Mailserver Security Assessment	Phish Alert	Ransomware Simulator
Weak Password Test	Phishing Security Test	Second Chance	Email Exposure Check Pro	Training Preview	Breached Password Test

Whitepapers

Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.
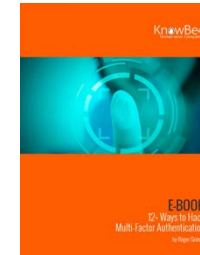
12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

» Learn More at www.KnowBe4.com/Resources «

Questions?

Bill Hardin – Vice President, Charles River Associates

BHardin@crai.com
Office: 312-619-3309

Roger A. Grimes – Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com