KnowBe4
Human error. Conquered.

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

John Mullen
Breach Coach
Mullen Coughlin

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

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

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

About Roger

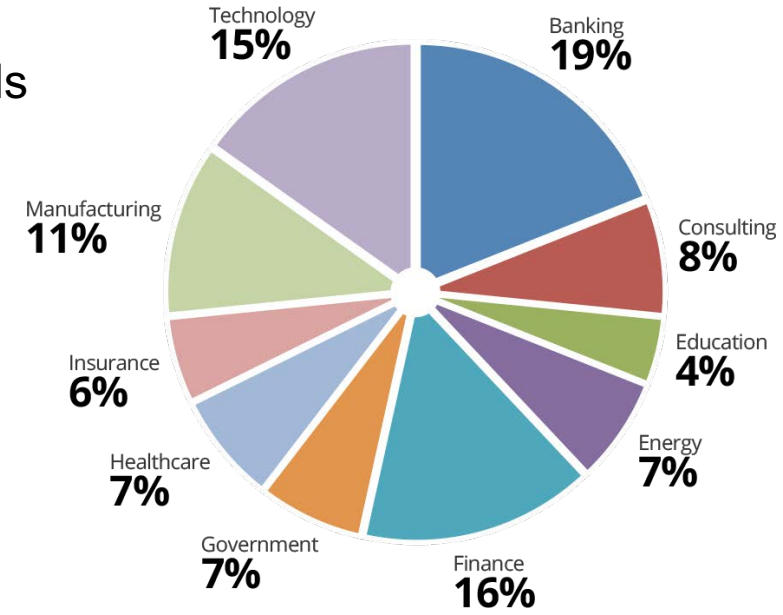
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 11 books and over 1,000 magazine articles
- *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



John Mullen, Sr.
Breach Coach
Named Partner & Founder
Mullen Coughlin

jmullen@mullen.law
267-930-4778 Office

About John

- Licensed as lawyer in Pennsylvania and New Jersey since 1991
- He regularly presents on data privacy and network security issues for insurers and brokers
- Published and quoted as a national expert on cyber/data loss issue
- Mr. Mullen and the firm focus their practice on assisting insureds in preparing for and responding to data privacy and network security events.

Mullen Coughlin LLC

- www.mullen.law
- Ph: 267-930-4778
- Founded by John Mullen, Jim Prendergast, Chris Dilenno, and Jennifer Coughlin.
- Mullen Coughlin is a law firm **uniquely dedicated** to solely servicing organizations of every size and from **every industry** with **data privacy** crises, incidents, and risks.
- 55 attorneys (and growing) uniquely focused on providing tailored data privacy and incident response services, including pre-breach planning and compliance, breach response, regulatory investigation and management, and privacy litigation defense under the umbrella of cyber insurance.

Agenda

Two-Part Webinar

Today

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

May 20th

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

Agenda

Q&A

Anatomy of a Breach Response

BREACH DISCOVERY

EXPERTS

- Breach coach
- Forensics
- Public relations

INVESTIGATION - internal/forensic/criminal

- How did it happen?
- When did it happen?
- Is it still happening?
- Who did it happen to?
- What was accessed/acquired? (What wasn't?)

NOTICE OBLIGATIONS

- State
- Federal
- Other (i.e. PCI)
- Deadlines – Can be 48 hours

NOTIFICATION

PROCESS

- Written
- Electronic
- Substitute
- To Media

VENDORS

- Printing, Mailing and Call Center
- Credit Monitoring

INQUIRIES

- State Regulators (i.e. AG, PD)
- Federal Regulators (i.e. OCR)
- Federal Agencies (i.e. SEC, FTC)
- Consumer reporting agencies
- Potential Plaintiffs

LITIGATION

- Government Entities
- Class Action
- Indemnification

Best Practices Post-Incident

- **Ensure experience on Response Team**
  - Post data incident is not the time to learn the ins and outs of incident response
  - Establish **Incident Response Team** of decision-makers (if not established already) as things move too fast for typical bureaucracy
- **Use Counsel to Establish Privilege**
  - Counsel directs forensics, notice drafting, and other vendors so that, in the event of litigation or regulatory investigation, all documents and communications are not discoverable
  - Guard Attorney-Client Privilege: **do not** share forensic reports, legal analysis and drafts with clients or third parties if not absolutely necessary
- Do not **use terms "Breach" or "PII" or "PHI" lightly** — these are statutorily defined legal terms the use and admission of which have consequences

Best Practices Post-Incident

- **Do not rush to go public**
  - Tremendous desire to go public fast, but an inability to answer questions that will inevitably follow can be devastating
  - **If your notice goes out 4 hours after discovery, there will be people who charge you with delay, so "delay" is unavoidable**
- **Prepare for litigation** and regulatory investigation — Preserve all relevant documents
- Conduct **risk assessment** and implement **data security improvements** prior to being asked by a regulator

Best Practices Pre-Incident

- **Empower** the organization's First Responders
- **Talk** to your IT Security folks. Gain an appreciation of the many challenges and risk landscape
  - Not many Firms can say: how many records they have; what type of data is being collected, stored, shared, protected; where does all this data reside; when is it purged?
- **Assess and test the organization's** staff and operations
- Prepare and **test your incident response plan**
- **Document** your due care measures (training and enforcement) being taken
- **Insure** yourself
- Repeat

Customers Are Building a Modern Security Stack….

People

Infrastructure

Devices

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.

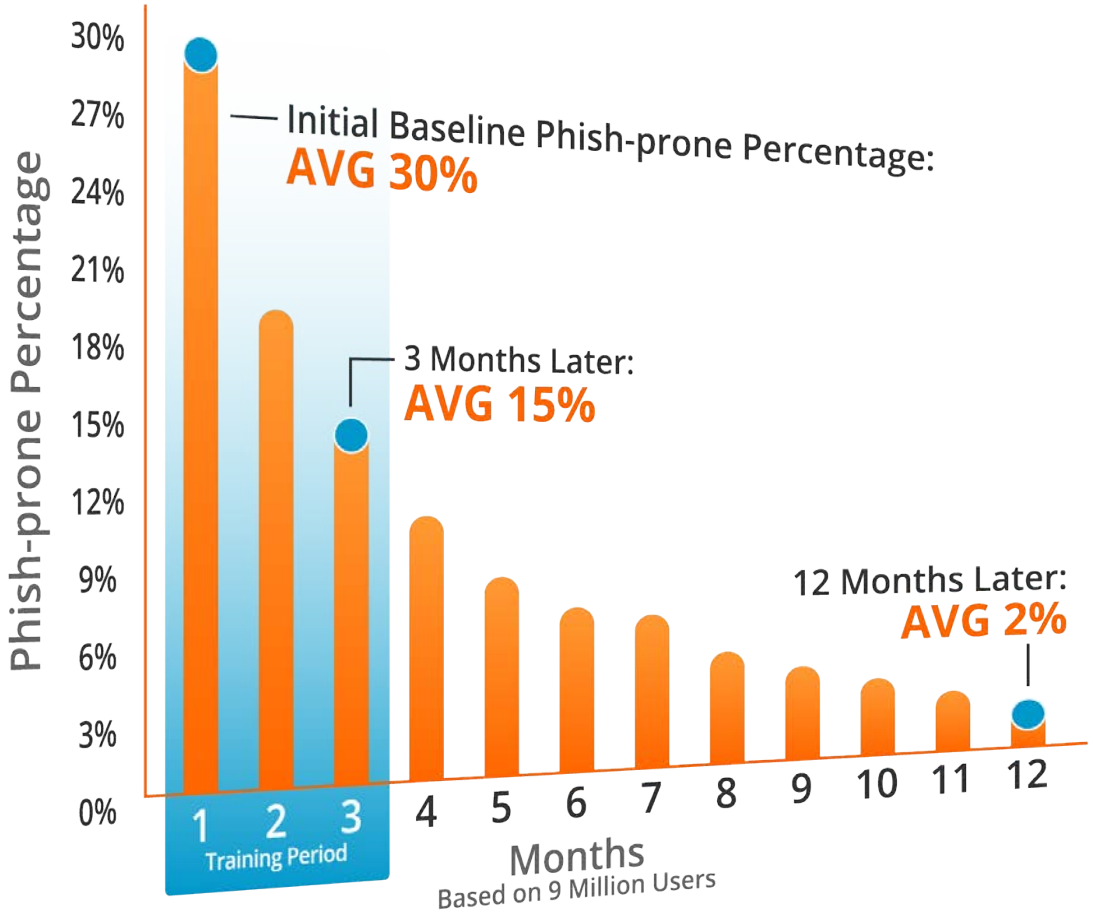
Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

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!

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)

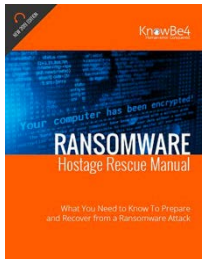


Resources

Free IT Security Tools

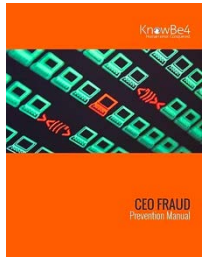
- Domain Doppelgänger
- Awareness Program Builder
- Domain Spoof Tool
- Mailserver Security Assessment
- Phish Alert
- Ransomware Simulator
- Weak Password Test
- Phishing Security Test
- Second Chance
- Email Exposure Check Pro
- Training Preview
- Breached Password Test

Whitepapers



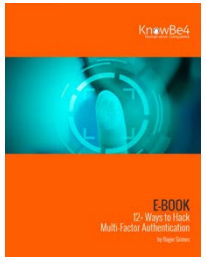
Ransomware Hostage Rescue Manual

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?

John Mullen- jmullen@mullen.law, 267-930-4778 Office

Roger A. Grimes- Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes, https://www.linkedin.com/in/rogeragrimes/

Don’t Forget Part II of this webinar series with Bill Hardin
On May 20th