Building and Updating an Incidence Response Plan

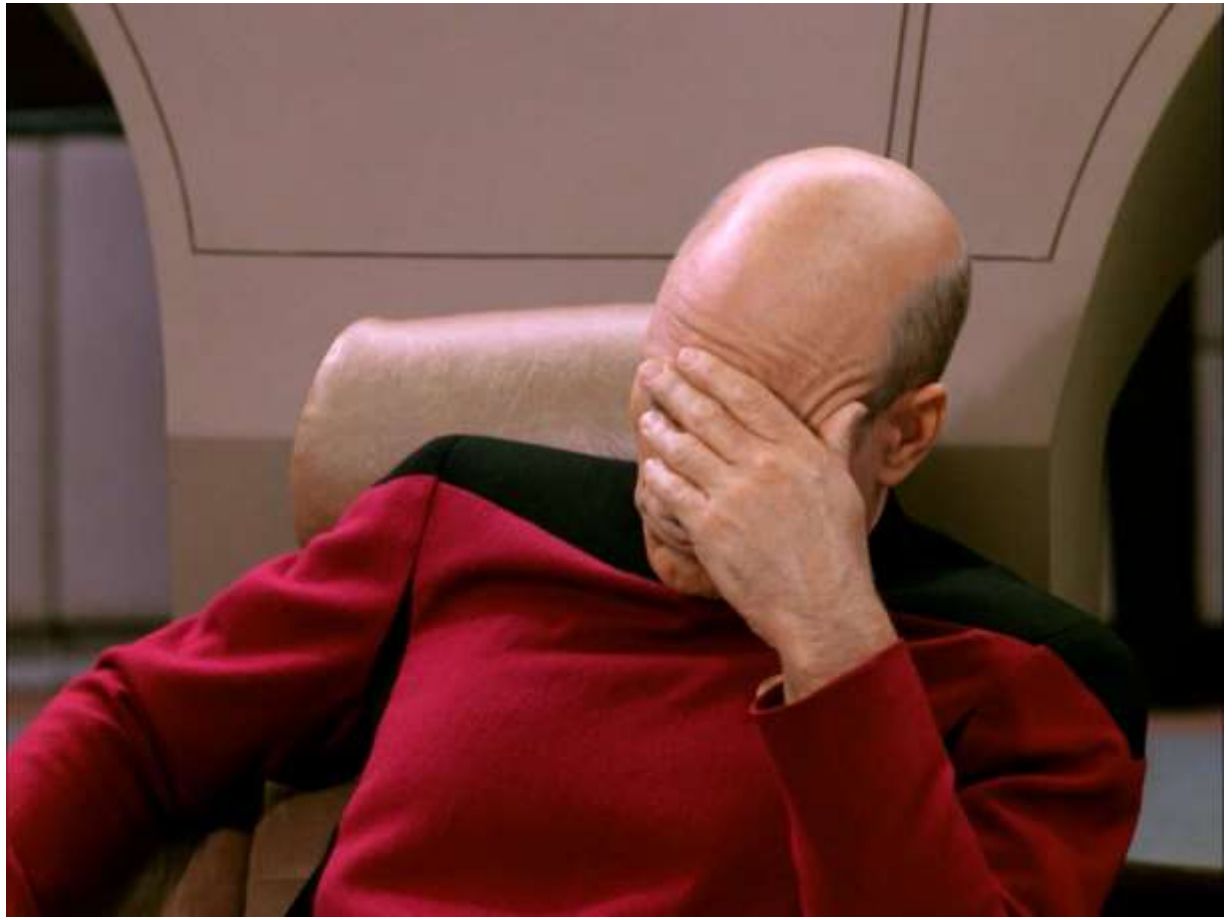
Jason Smith
Security & Compliance Consultant
Internetwork Engineering

HIMSS NORTH CAROLINA Chapter

The average time between an attacker breaching a network and its owner noticing the intrusion is

150 days.

How is your IR Process



Incident Response Maturity Levels

Maturity Level		Ad-hoc		Maturing		Strategic
		As Needed	Dedicated Part-Time	Full-Time	SOC/IR+	Fusion
Existing IR Capabilities	People	▪ 0-1	▪ 1-3 ▪ Specialization	▪ 2-5 ▪ Formal roles	▪ ~10 ▪ Shifts (24x7)	▪ 15+ ▪ Intel, SOC, and IR Teams
	Process	▪ Chaotic and relying on individual heroics; reactive ▪ General purpose run-book ▪ Tribal knowledge	▪ Situational run books; some consistency ▪ Email-based processes	▪ Requirements and Workflows documented as standard business process ▪ Some improvement over time	▪ Process is measured via metrics ▪ Minimal Threat Sharing ▪ Shift turnover ▪ SLAs	▪ Processes are constantly improved and optimized ▪ Broad Threat sharing ▪ Hunt teams
	Technology	▪ AV ▪ Firewalls ▪ IDS/IPS	▪ SIEM ▪ Sandboxing	▪ Continuous Monitoring ▪ Endpoint Forensics ▪ Tactical Intelligence	▪ Malware Analysis ▪ Additional Intelligence ▪ IT Operations Integration	▪ Intel+Incident Response Drives Security Program ▪ Strategic Intelligence ▪ Coordination with Physical Security/Intelligence
CMM Equivalent		Initial	Repeatable	Defined	Managed	Optimized

Slower Response = Greater Risk

66%
of breaches took months or even years to discover

60%
of breaches have data exfiltrated in first 24 hours

60,000
Number of alerts hackers set off at Global Retailer

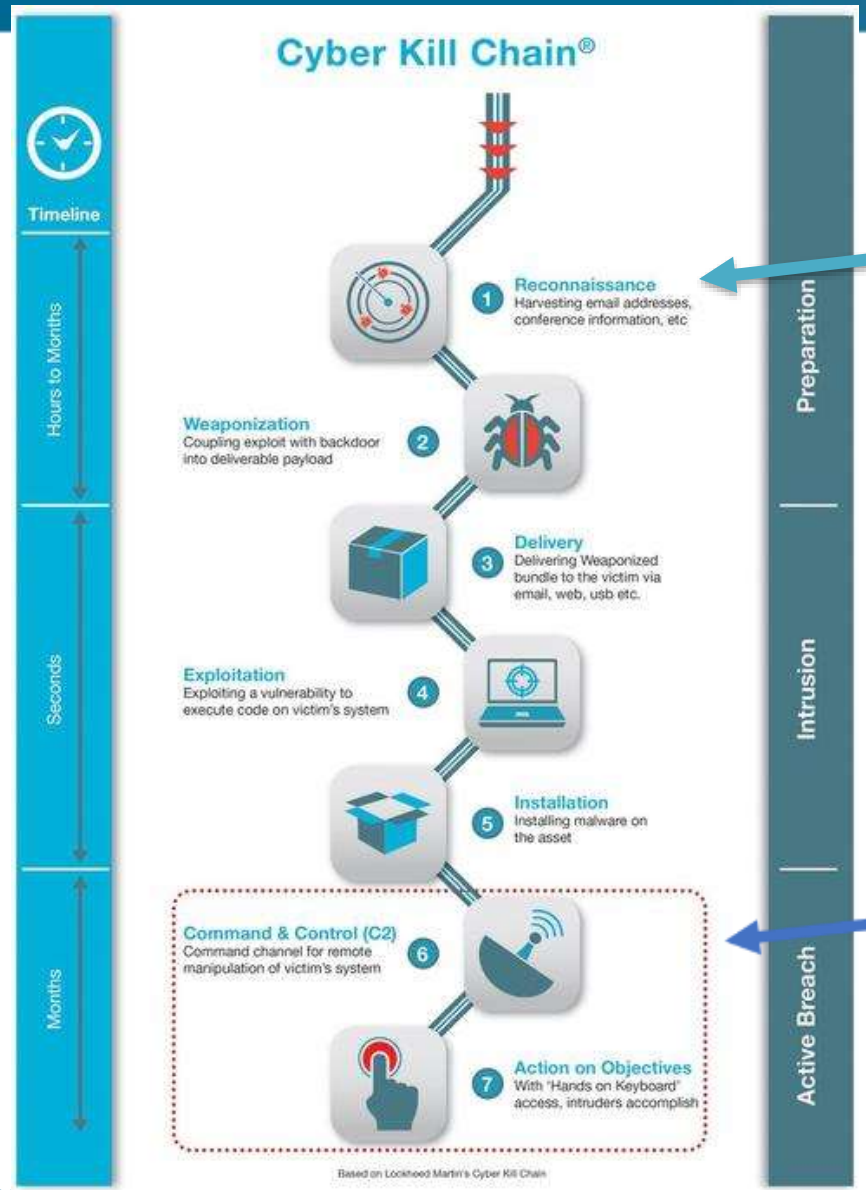
229
Median number of days advanced attackers present before detection

33%
Of organizations discover breaches through their own monitoring

Why Security Approaches Fail

- It is not a fair fight to begin with
- Bad guys have the economic advantage
- People, Process and Technology Issues
- **Security Technology Issues**
- **Silo'ed Point Products that do not work together**
- Bolt on security, static and not integrated
- We are designing in complexity on purpose!
- **Hyper focus on Product**
- To much noise, complexity, expertise = unstainable posture

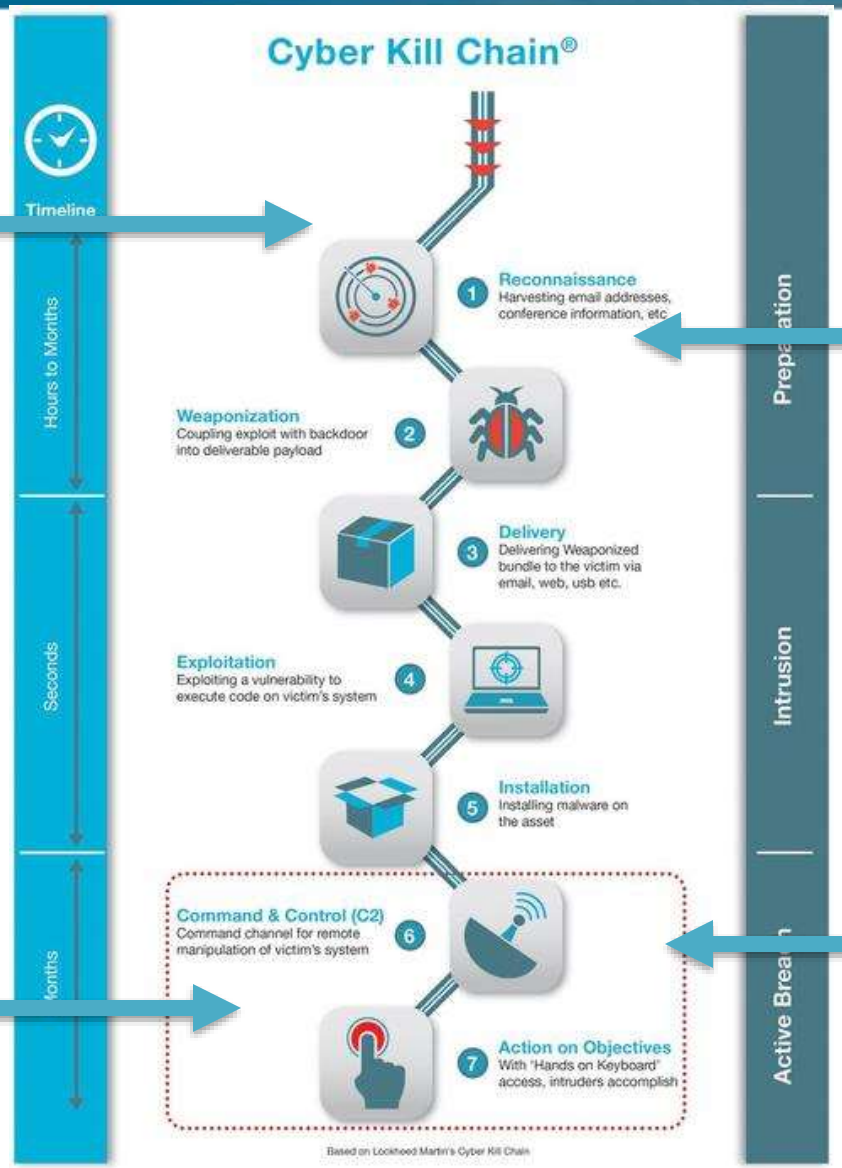
The Cyber Kill Chain



Hopefully, you are here.

Hopefully, you are NOT here.

Addressing the Threat

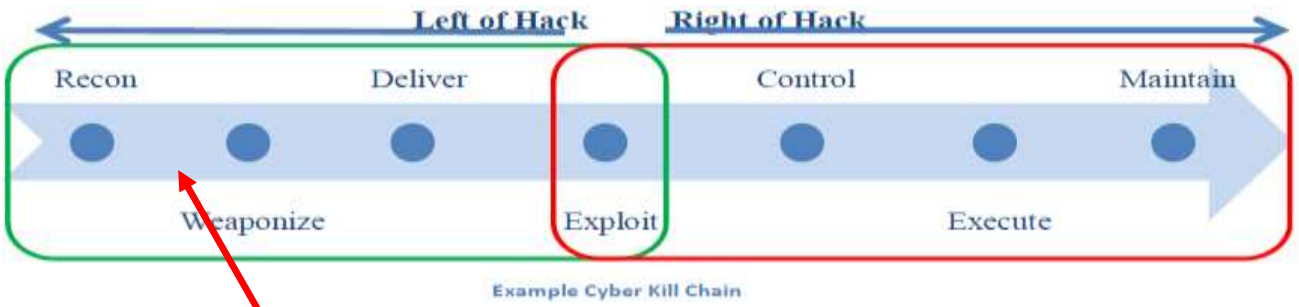


Look Familiar?

Incident Response & Vulnerability Management

Malware Exploits Vulnerabilities

More Vulnerabilities = Larger Attack Surface



Opportunity

Decrease Number of Vulnerabilities

Reduce the Attack Surface

HIMSS NORTH CAROLINA Chapter

tenable network security

IR & The Kill Chain

Incident Response

1st Step – Risk Assessment

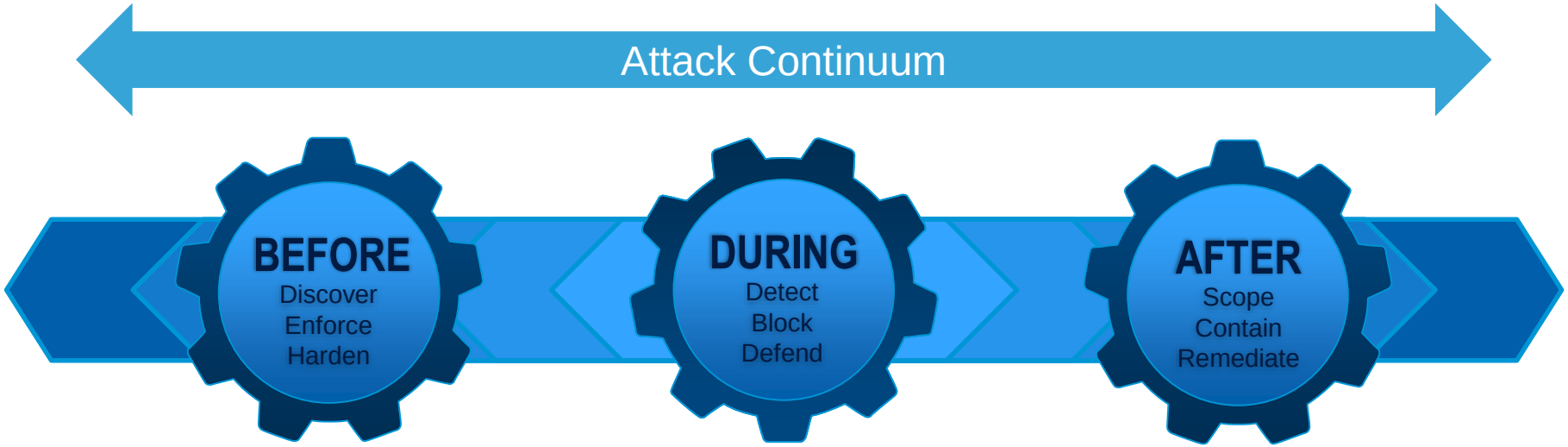
Identify the sources of Risk

What is the Impact (to the business)

Develop a Risk Reduction and Mitigation Strategy

Define it in Policy, Processes, and Procedures

Keep it Simple



Damage Control

Goal: Return the business to it's operational mission, learn, implement compensating controls.

- **Scope** – Determine just how bad a breach is. Assess it's impact and know how to prioritize your efforts. (Do you know what types of data is on the affected servers?)
- **Contain** – Lock it down. No matter how bad it is, if it spreads, it will only be worse.
- **Remediate** – Clean up and get back to business. But don't just "remove" the bad, learn from it and implement compensating controls (BEFORE the next attack).

Plan the Work, Work the Plan!

- Documentation
  - Record dates and times
  - Who, what, when, where, why
- Activate the IR Team
- Secure the Scene
  - Evidence preservation
  - Chain of custody

Lock Down the Affected Assets

- Take offline, but leave on

Interview those involved

Priorities and Risks

Forensics team deployment

Notify Law Enforcement

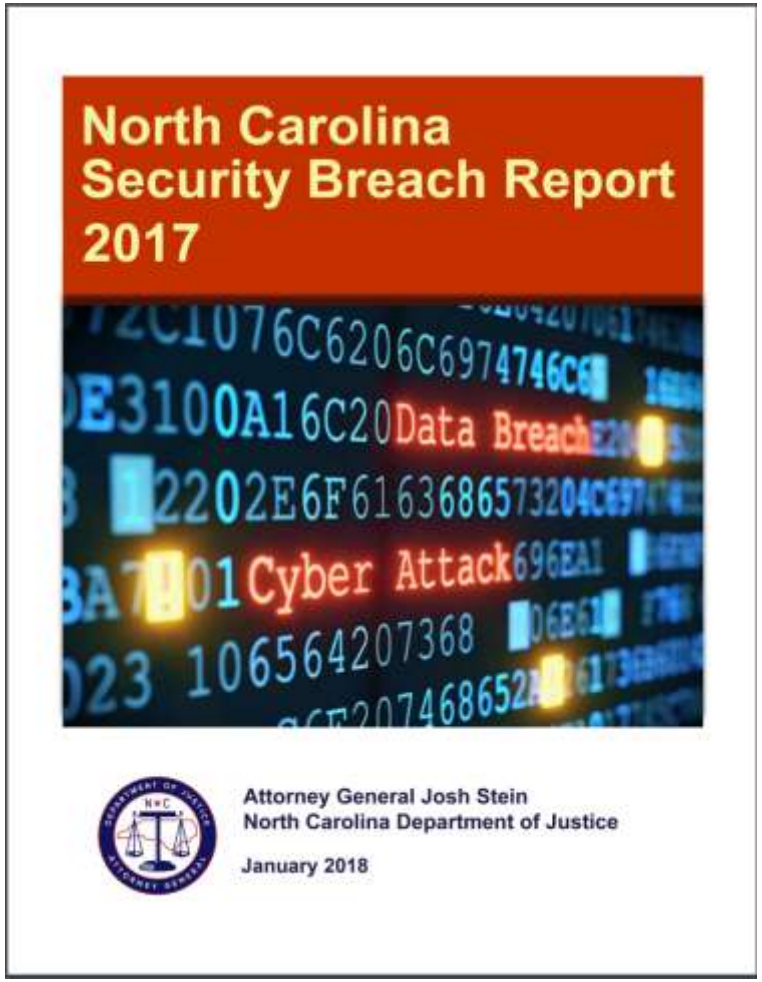
IR Process

- IR Team touch points cadence
- Remediation
- Forensic Review
- Notifications (Legal)
  - Data Breach Notification Vendor
  - Breach Insurance vendor
- C-Suite Updates

Be Prepared!

- Develop (and Test) an Incident Response Plan
  - Notification Process?
  - What are the legal obligations?
- Build an IR Team
  - Who is in charge?
- Measure effectiveness of Security Controls
  - Adequately staffed and trained?
  - Repeatable processes?
  - Logging and alerting?
- Refine process and test routinely

New North Carolina Breach Law



- New Sense of Urgency!
- Changes:
- New Definition of Breach.
  - Unauthorized access or acquisition
- Shortened Notification Period
  - 15 days to notify the affected party and the NC AG's office
- "Reasonable Safeguard" Requirements
  - Security controls
- Strengthen Penalty Provisions
  - $5000 per record affected

Improve? - Time to Practice

- Assess, Plan, Acquire, Test, Repeat
- OODA Loops
  - Observe, Orient, Decide, Act
- Use your Risk Management Process and current Risk Assessment as a reference guide
- Revisit IR Plan frequently
- Practice, Practice, Practice

Incident Response Services

Two Options:

Roll Your Own IR Program

- Benefits: scalable to your organization, maybe cheaper
- Challenges: difficult to maintain readiness, may not be cheaper

IR as a Service

- Benefits: maybe cheaper, well defined, proven results
- Challenges: initial and recurring expense justification

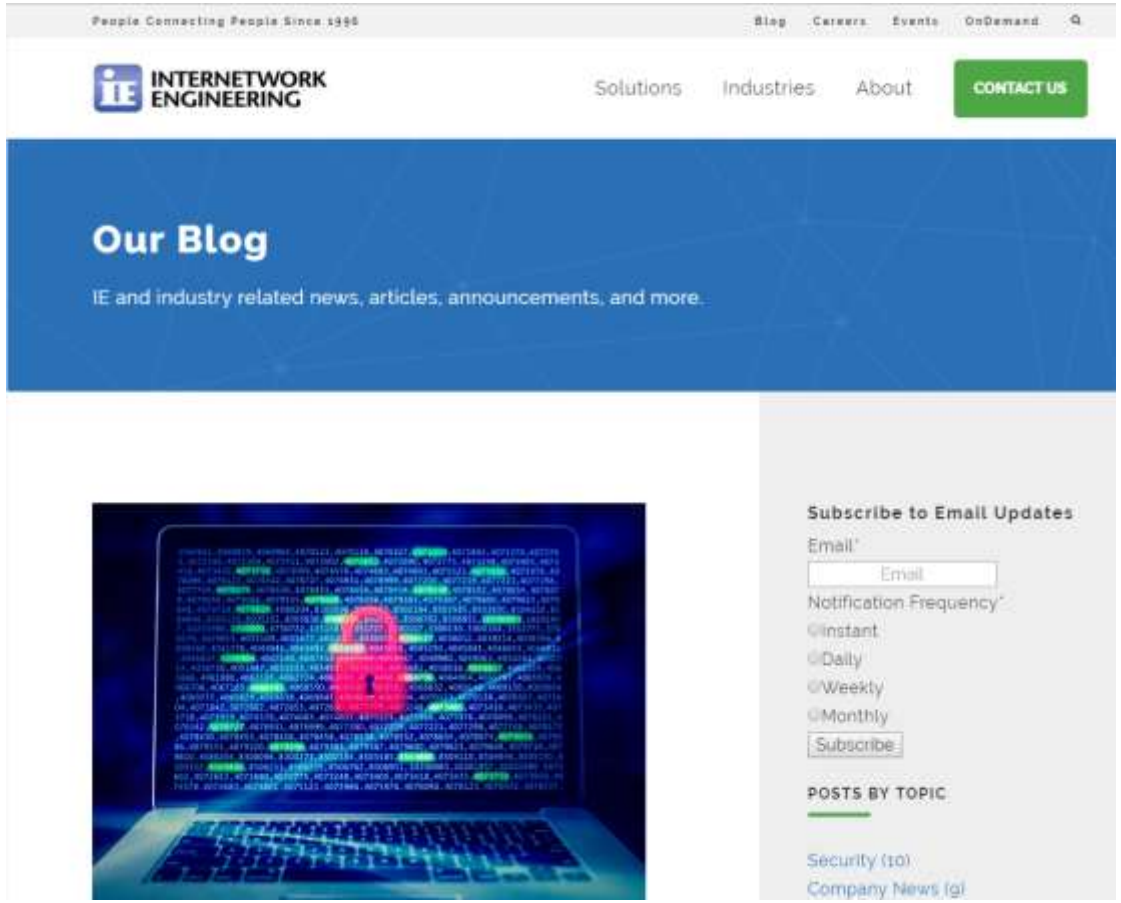
Questions??

Security User Groups

Meet Quarterly:
Charlotte NC,
Raleigh NC

Coming Soon:
Columbia SC
Knoxville TN

Check out our Blog!



New Website!

Subscribe to our Security Blog

Check for events

Thank you!

Jason Smith
jsmith@ineteng.com
704-943-9835
@smith380