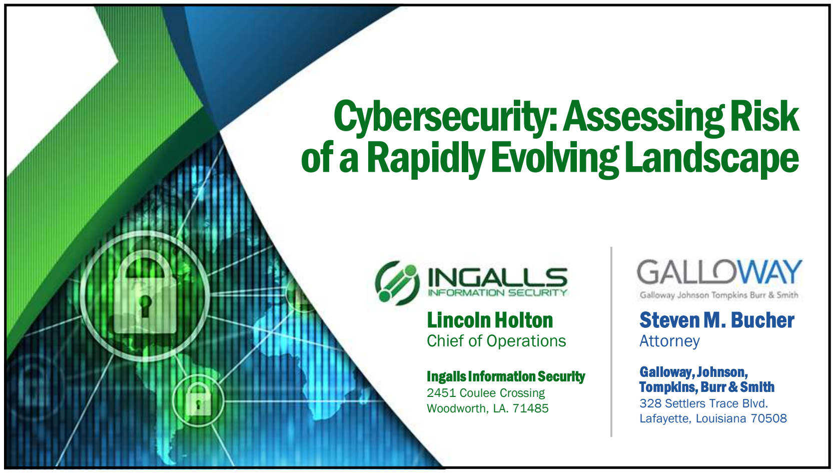


Cybersecurity: Assessing Risk of a Rapidly Evolving Landscape

INGALLS INFORMATION SECURITY

Lincoln Holton
Chief of Operations

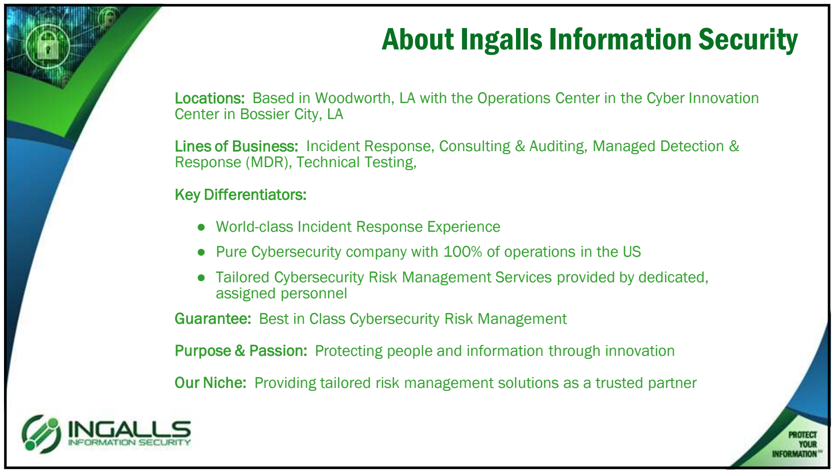
Ingalls Information Security
2451 Coulee Crossing
Woodworth, LA. 71485

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

Steven M. Bucher
Attorney

Galloway, Johnson, Tompkins, Burr & Smith
328 Settlers Trace Blvd.
Lafayette, Louisiana 70508

1



About Ingalls Information Security

Locations: Based in Woodworth, LA with the Operations Center in the Cyber Innovation Center in Bossier City, LA

Lines of Business: Incident Response, Consulting & Auditing, Managed Detection & Response (MDR), Technical Testing,

Key Differentiators:

- World-class Incident Response Experience
- Pure Cybersecurity company with 100% of operations in the US
- Tailored Cybersecurity Risk Management Services provided by dedicated, assigned personnel

Guarantee: Best in Class Cybersecurity Risk Management

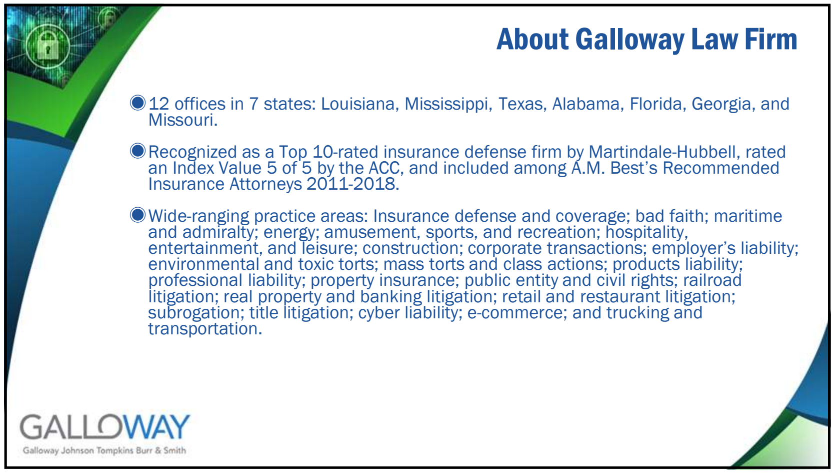
Purpose & Passion: Protecting people and information through innovation

Our Niche: Providing tailored risk management solutions as a trusted partner

INGALLS INFORMATION SECURITY

PROTECT YOUR INFORMATION™

2



About Galloway Law Firm

- 12 offices in 7 states: Louisiana, Mississippi, Texas, Alabama, Florida, Georgia, and Missouri.
- Recognized as a Top 10-rated insurance defense firm by Martindale-Hubbell, rated an Index Value 5 of 5 by the ACC, and included among A.M. Best's Recommended Insurance Attorneys 2011-2018.
- Wide-ranging practice areas: Insurance defense and coverage; bad faith; maritime and admiralty; energy; amusement, sports, and recreation; hospitality, entertainment, and leisure; construction; corporate transactions; employer's liability; environmental and toxic torts; mass torts and class actions; products liability; professional liability; property insurance; public entity and civil rights; railroad litigation; real property and banking litigation; retail and restaurant litigation; subrogation; title litigation; cyber liability; e-commerce; and trucking and transportation.

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

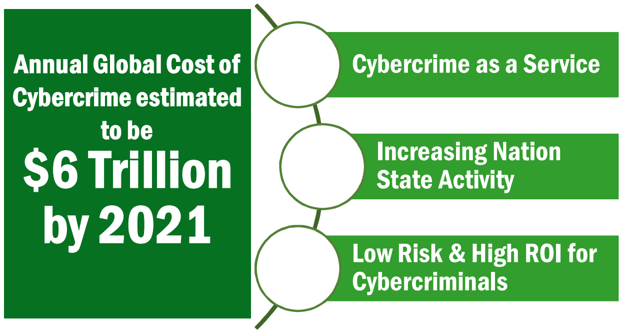
3

What is at stake?

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

4

Cybercrime



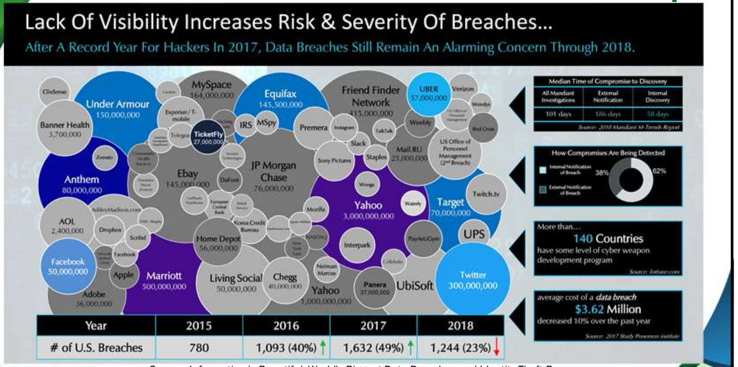
Annual Global Cost of Cybercrime estimated to be

$6 Trillion by 2021

- Cybercrime as a Service
- Increasing Nation State Activity
- Low Risk & High ROI for Cybercriminals

5

2018 Threat Landscape



Lack Of Visibility Increases Risk & Severity Of Breaches…

After A Record Year For Hackers In 2017, Data Breaches Still Remain An Alarming Concern Through 2018.

Year	2015	2016	2017	2018
# of U.S. Breaches	780	1,093 (40%) ↑	1,632 (49%) ↑	1,244 (23%) ↓

Median Time of Compromise to Discovery

All Mandiant Investigations	External Notification	Internal Discovery
101 days	186 days	58 days

Source: 2018 Mandiant M-Trends Report

How Compromises Are Being Detected

Internal Notification of Breach
External Notification of Breach
38%
62%

More than… 140 Countries have some level of cyber weapon development program

Source: fortune.com

average cost of a *data breach* $3.62 Million decreased 10% over the past year

Source: 2017 Study Ponemon institute

Source: Information is Beautiful: World's Biggest Data Breaches and Identity Theft Resource Center (ITRC): 2018 Annual Data Breach Year-End Review. Information as of December 31, 2018.

6

Cybercrime Trends

Ooops, your files have been encrypted!

Ransomware attack

Phishing is The Common Element

Training employees on how to recognize and react to phishing emails and cyber threats is one of the best security ROI

7

Why do Social Engineering tactics work?

The Amygdala is part of the brain that is largely responsible for generating emotional responses. When humans are presented with something that is threatening or overwhelming, the amygdala hijacks the rationale brain, often leading to irrational decision making.

Social Engineering tactics prey on your emotions!

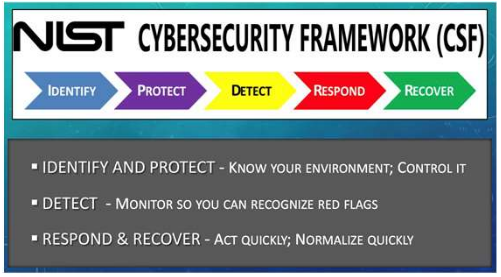
8

Managing Your Risk

9

Managing Risk

- Risk is part of life and business.
  - We need to be aware of our risks, decide on what level of risk we can accept, and have plans in place for when things go wrong


NIST CYBERSECURITY FRAMEWORK (CSF)

- IDENTIFY AND PROTECT - KNOW YOUR ENVIRONMENT; CONTROL IT
- DETECT - MONITOR SO YOU CAN RECOGNIZE RED FLAGS
- RESPOND & RECOVER - ACT QUICKLY; NORMALIZE QUICKLY

10

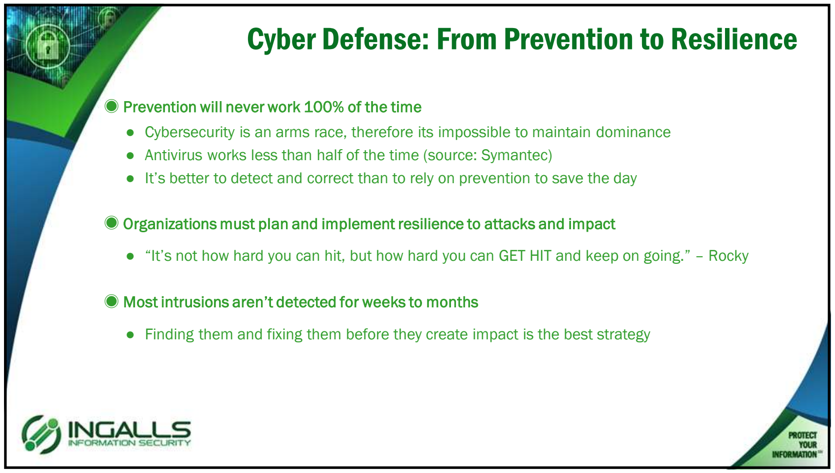
Legal Considerations

11

Cyber Defense: From Prevention to Resilience

- Prevention will never work 100% of the time
  - Cybersecurity is an arms race, therefore its impossible to maintain dominance
  - Antivirus works less than half of the time (source: Symantec)
  - It's better to detect and correct than to rely on prevention to save the day
- Organizations must plan and implement resilience to attacks and impact
  - "It's not how hard you can hit, but how hard you can GET HIT and keep on going." – Rocky
- Most intrusions aren't detected for weeks to months
  - Finding them and fixing them before they create impact is the best strategy

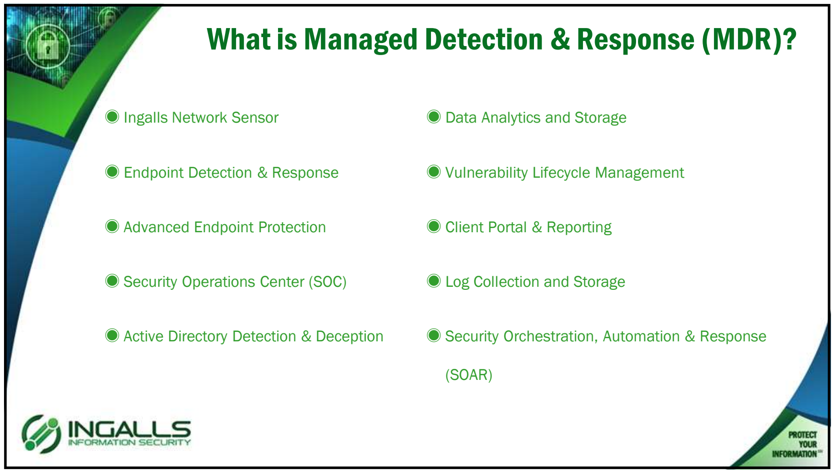
12



Cyber Defense: From Prevention to Resilience

- Prevention will never work 100% of the time
  - Cybersecurity is an arms race, therefore its impossible to maintain dominance
  - Antivirus works less than half of the time (source: Symantec)
  - It's better to detect and correct than to rely on prevention to save the day
- Organizations must plan and implement resilience to attacks and impact
  - "It's not how hard you can hit, but how hard you can GET HIT and keep on going." – Rocky
- Most intrusions aren't detected for weeks to months
  - Finding them and fixing them before they create impact is the best strategy

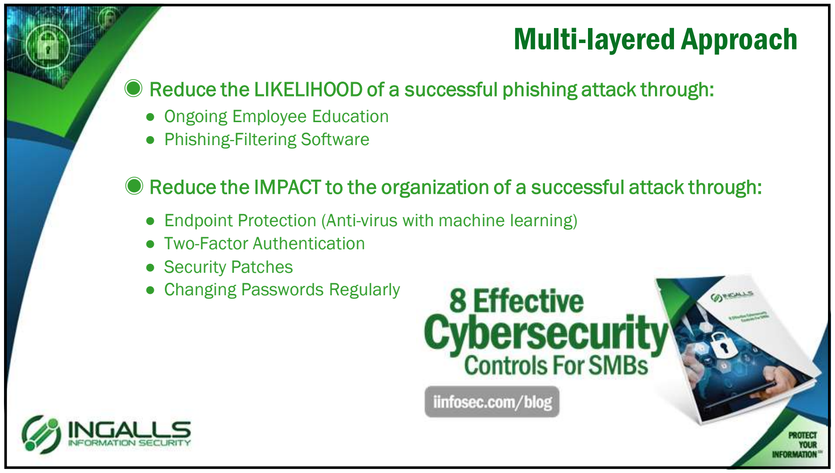
13



What is Managed Detection & Response (MDR)?

- Ingalls Network Sensor
- Endpoint Detection & Response
- Advanced Endpoint Protection
- Security Operations Center (SOC)
- Active Directory Detection & Deception
- Data Analytics and Storage
- Vulnerability Lifecycle Management
- Client Portal & Reporting
- Log Collection and Storage
- Security Orchestration, Automation & Response (SOAR)

14



Multi-layered Approach

- Reduce the LIKELIHOOD of a successful phishing attack through:
  - Ongoing Employee Education
  - Phishing-Filtering Software
- Reduce the IMPACT to the organization of a successful attack through:
  - Endpoint Protection (Anti-virus with machine learning)
  - Two-Factor Authentication
  - Security Patches
  - Changing Passwords Regularly

8 Effective Cybersecurity Controls For SMBs

iinfosec.com/blog

15

Corporate Governance

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

16

Insurance

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

17

Questions?

INGALLS
INFORMATION SECURITY

Lincoln Holton

(888) 860-0452
lincoln.holton@iinfosec.com

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

Steven M. Bucher

(337) 735-1760
sbucher@gallowaylawfirm.com

18