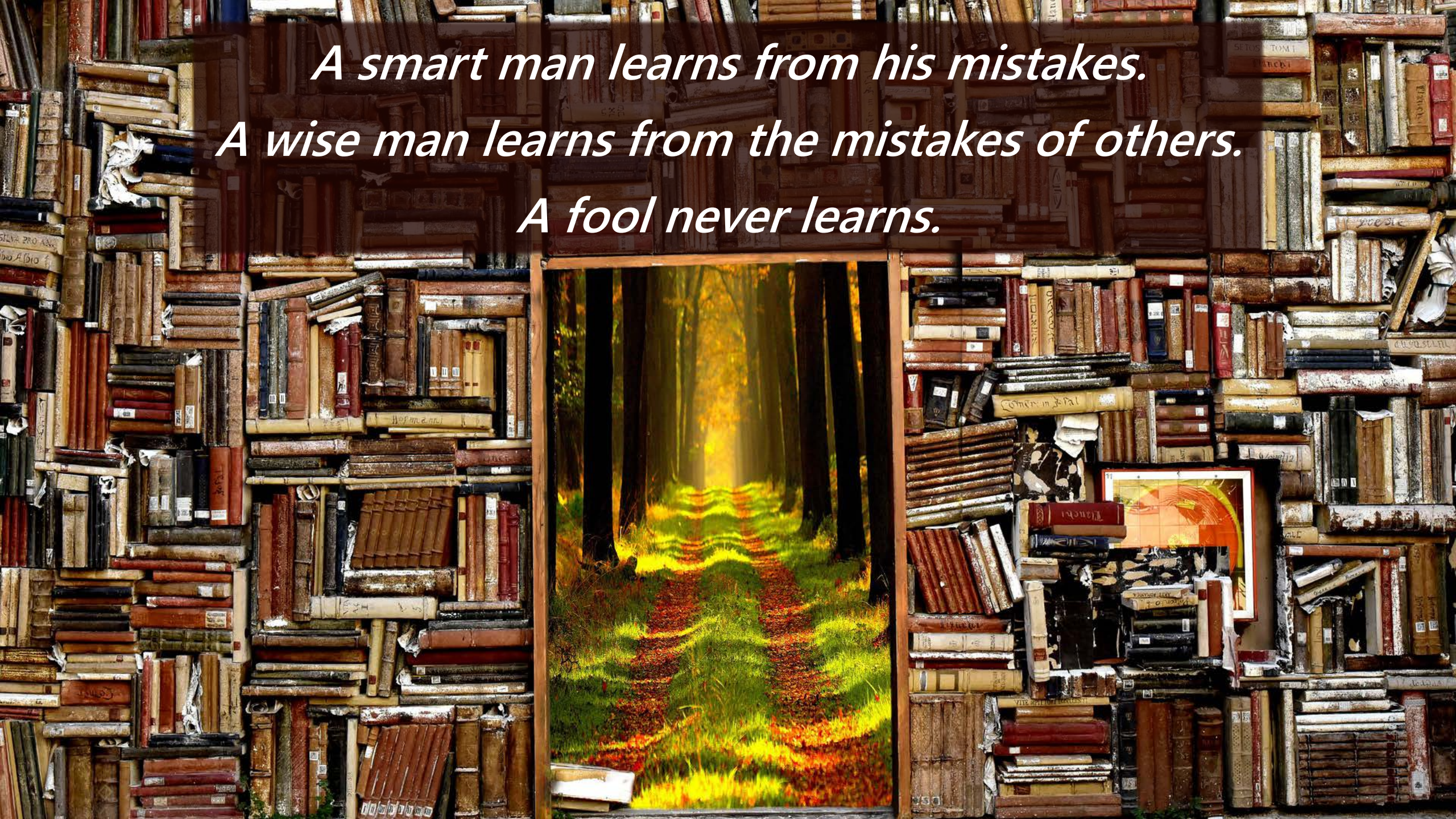
The Legal Case for Cybersecurity

Why Companies Need a Cyber Risk Management Program and How to Develop and Mature Them

Shawn E. Tuma
Cybersecurity & Data Privacy Attorney
Scheef & Stone, LLP
Shawn.Tuma@solidcounsel.com
(214) 472-2135
@shawnetuma

SCHEEF & STONE
SOLID COUNSEL


A smart man learns from his mistakes.
A wise man learns from the mistakes of others.
A fool never learns.


Neiman Marcus
SuperValu
Real Food, Real People
SONY
Michaels
STAPLES
AdultFriendFinder
ASHLEY MADISON
Life is short. Have an affair.
Get started by telling us your relationship status:
Please Select
See Your Matches»
Over 22,995,000 anonymous
CHIPOTLE
MEXICAN GRILL
EQUIFAX
YAHOO!
ups
SALLY BEAUTY SUPPLY
SONIC
TE LODGING


Cybersecurity is no longer just an IT issue—
it is an overall business risk issue.


Security and IT protect companies' data;
Legal protects companies *from* their data.

Laws and regulations

- Types
  - Security
  - Privacy
  - Unauthorized Access
- International Laws
  - Privacy Shield
  - GDPR
- Federal Laws & Regs.
  - HIPAA, GLBA, FERPA
  - FTC, SEC, FCC, HHS
- State Laws
  - 48 states (AL & SD)
  - NYDFS & Colorado FinServ
- Industry Groups
  - PCI, FINRA
- Contracts
  - 3rd Party Bus. Assoc.
  - Data Security Addendum

Usually the real-world threats are not so sophisticated

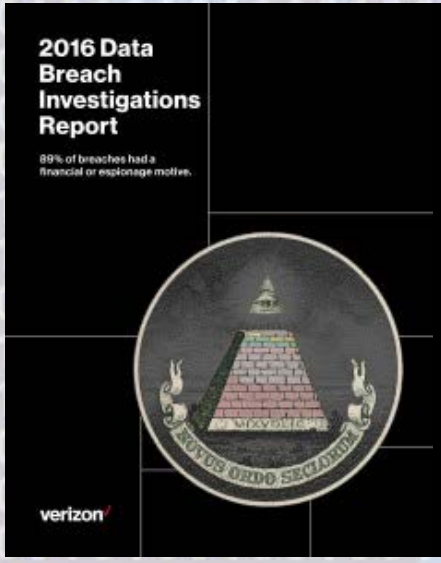
Easily Avoidable Breaches

90% in 2014

91% in 2015

91% in 2016 (90% from email)

OTA
Online Trust Alliance



- 63% confirmed breaches from weak, default, or stolen passwords
- Data is lost over 100x more than stolen
- Phishing used most to install malware

SCHEEF & STONE
SOLID COUNSEL

shawnetuma.com
"Publications" tab

SCHEEF & STONE
SOLID COUNSEL

Good Cyber Hygiene Checklist

GOOD CYBER HYGIENE

- ❑ Start with a risk assessment
- ❑ Written policies and procedures focused on cybersecurity and tailored to company
  - Expectations for protection of data
  - Monitoring and expectations of privacy
  - Confidentiality of data
  - Limits of permissible access and use
  - Social engineering
  - Passwords policy & security questions
  - BYOD
- ❑ Training of all workforce on your policies and procedures, first, then security training
- ❑ Phish all workforce (incl. upper management)
- ❑ Multi-factor authentication
- ❑ Signature based antivirus and malware detection
- ❑ Internal controls / access controls
- ❑ No default passwords
- ❑ No outdated or unsupported software
- ❑ Security patch updates management policy
- ❑ Backups: segmented offline, cloud, redundant
- ❑ Use reputable cloud services
- ❑ Encrypt sensitive data and air-gap hypersensitive data
- ❑ Adequate logging and retention
- ❑ Incident response plan
- ❑ Third-party security risk management program
- ❑ Firewall, intrusion detection, and intrusion prevention systems
- ❑ Managed services provider (MSP) or managed security services provider (MSSP)
- ❑ Cyber risk insurance

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a **comprehensive information security program** that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondents' or the business entity's size and complexity, the nature and scope of respondents' or the business entity's activities, and the sensitivity of the personal information collected from or about consumers." *In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014).*

"[T]he relevant inquiry here is a cost-benefit analysis, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." *FTC v. Wyndham*, (3rd Cir. Aug. 24, 2015)

For more information, please contact:
Shawn E. Tuma
Cybersecurity & Data Privacy Attorney
Direct: 214.472.2135 | Mobile: 214.726.2808
shawn.tuma@solidcounsel.com
Blog: www.shawnetuma.com

Common Cybersecurity Best Practices

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
   - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Managed services provider (MSP) or managed security services provider (MSSP).
17. Cyber risk insurance.

SCHEEF & STONE
SOLID COUNSEL

Does your company have *reasonable* cybersecurity?

In re Target Data Security Breach Litigation, (Financial Institutions) (Dec. 2, 2014)

F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. Aug. 24, 2015)

SCHEEF & STONE
SOLID COUNSEL

1. **Risk assessment.**
2. **Policies and procedures focused on cybersecurity.**
   - **Social engineering, password, security questions**
3. **Training of all workforce on P&P, then security.**
4. **Phish all workforce (esp. leadership).**
5. **Multi-factor authentication.**
6. **Signature based antivirus and malware detection.**
7. **Internal controls / access controls.**
8. **No outdated or unsupported software.**
9. **Security patch updates management policy.**
10. **Backups segmented offline, cloud, redundant.**
11. **Incident response plan.**
12. **Encrypt sensitive and air-gap hypersensitive data.**
13. **Adequate logging and retention.**
14. **Third-party security risk management program.**
15. **Firewall, intrusion detection and prevention systems.**
16. Managed services provider (MSP) or managed security services provider (MSSP).
17. Cyber risk insurance.

Does your company have adequate internal network controls?

FTC v. LabMD, (July 2016 FTC Commission Order)

SCHEEF & STONE
SOLID COUNSEL

1. **Risk assessment.**
2. **Policies and procedures focused on cybersecurity.**
   - Social engineering, password, security questions
3. **Training of all workforce on P&P, then security.**
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature based antivirus and malware detection.
7. **Internal controls / access controls.**
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Managed services provider (MSP) or managed security services provider (MSSP).
17. Cyber risk insurance.

Does your company have written policies and procedures focused on cybersecurity?

SEC v. R.T. Jones Capital Equities Mgt., Consent Order (Sept. 22, 2015)

SCHEEF & STONE
SOLID COUNSEL

1. Risk assessment.
2. **Policies and procedures focused on cybersecurity.**
   - **Social engineering, password, security questions**
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Managed services provider (MSP) or managed security services provider (MSSP).
17. Cyber risk insurance.

Does your company have a written cybersecurity incident response plan?

SEC v. R.T. Jones Capital Equities Mgt., Consent Order (Sept. 22, 2015)

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
   - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. **Incident response plan.**
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Managed services provider (MSP) or managed security services provider (MSSP).
17. Cyber risk insurance.

SCHEEF & STONE
SOLID COUNSEL

Does your company manage third-party cyber risk?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014)

SCHEEF & STONE
SOLID COUNSEL

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
   - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. **Third-party security risk management program.**
15. Firewall, intrusion detection and prevention systems.
16. Managed services provider (MSP) or managed security services provider (MSSP).
17. Cyber risk insurance.

How mature is your company's cyber risk management program?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014).

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondents' or the business entity's size and complexity, the nature and scope of respondents' or the business entity's activities, and the sensitivity of the personal information collected from or about consumers"

SCHEEF & STONE
SOLID COUNSEL

How mature is your company's cyber risk management program?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014).

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which –

(1) must be fully documented in writing,

SCHEEF & STONE
SOLID COUNSEL

How mature is your company's cyber risk management program?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014).

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which –

(1) must be fully documented in writing,

(2) shall contain administrative, technical, and physical safeguards

SCHEEF & STONE
SOLID COUNSEL

How mature is your company's cyber risk management program?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014).

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which –

(1) must be fully documented in writing,

(2) shall contain administrative, technical, and physical safeguards

(3) appropriate to respondents' or the business entity's

  (1) size and complexity,

SCHEEF & STONE
SOLID COUNSEL

How mature is your company's cyber risk management program?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014).

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which –

(1) must be fully documented in writing,

(2) shall contain administrative, technical, and physical safeguards

(3) appropriate to respondents' or the business entity's

  (1) size and complexity,

  (2) the nature and scope of respondents' or the business entity's activities, and

SCHEEF & STONE
SOLID COUNSEL

How mature is your company's cyber risk management program?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014).

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which –

(1) must be fully documented in writing,

(2) shall contain administrative, technical, and physical safeguards

(3) appropriate to respondents' or the business entity's

  (1) size and complexity,

  (2) the nature and scope of respondents' or the business entity's activities, and

  (3) the sensitivity of the personal information collected from or about consumers"

SCHEEF & STONE
SOLID COUNSEL

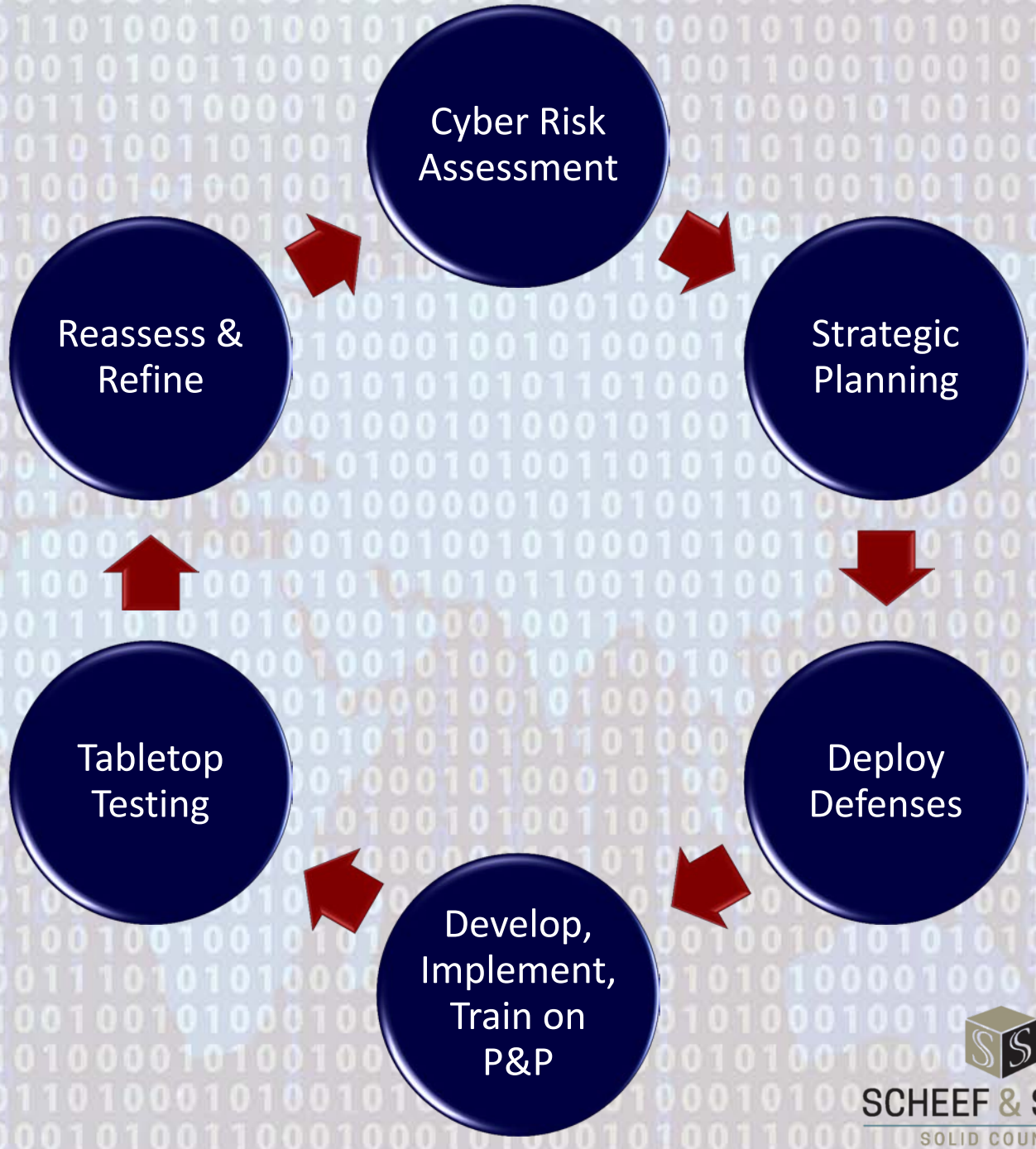
New York Department of Financial Services Cybersecurity (NYDFS) Requirements for Financial Services Companies + [fill in]

- All NY “financial institutions” + third party service providers.
- Third party service providers – examine, obligate, audit.
- Establish Cybersecurity Program (w/ specifics):
  - Logging, Data Classification, IDS, IPS;
  - Pen Testing, Vulnerability Assessments, Risk Assessment; and
  - Encryption, Access Controls.
- Adopt Cybersecurity Policies.
- Designate qualified CISO to be responsible.
- Adequate cybersecurity personnel and intelligence.
- Personnel Policies & Procedures, Training, Written IRP.
- Chairman or Senior Officer Certify Compliance.

EU – General Data Protection Regulation (GDPR)

- Goal: Protect all EU citizens from privacy and data breaches.
- When: May 25, 2018.
- Reach: Applies to all companies (controllers and processors):
  - Processing data of EU residents (regardless of where processing),
  - In the EU (regardless of where processing), or
  - Offering goods or services to EU citizens or monitoring behavior in EU.
- Penalties: up to 4% global turnover or €20 Million (whichever is greater).
- Remedies: data subjects have judicial remedies, right to damages.
- Data subject rights:
  - Breach notification – 72 hrs to DPA; “without undue delay” to data subjects.
  - Right to access – provide confirmation of processing and electronic copy (free).
  - Data erasure – right to be forgotten, erase, cease dissemination or processing.
  - Data portability – receive previously provided data in common elect. format.
  - Privacy by design – include data protection from the onset of designing systems.

Cyber Risk Management Program



SCHEEF & STONE
SOLID COUNSEL

shawnetuma.com
“Publications” tab

SCHEEF & STONE
SOLID COUNSEL

SCHEEF & STONE
SOLID COUNSEL

Data Breach Response Checklist

DATA BREACH INCIDENT RESPONSE

- ❑ Determine whether incident justifies escalation
- ❑ Begin documentation of decisions and actions
- ❑ Begin mitigation of compromise
- ❑ Engage experienced legal counsel to guide through process, determine privilege vs disclosure tracks
- ❑ Activate Incident Response Plan and notify and convene Incident Response Team
- ❑ Notify cyber insurance carrier
- ❑ Notify affected business partners per contractual obligations
- ❑ Engage forensics to mitigate continued harm, gather evidence, and investigate
- ❑ Assess scope and nature of data compromised
- ❑ Preliminarily determine legal obligations based on type of data and jurisdictions
- ❑ Determine whether to notify law enforcement
- ❑ Begin preparing public relations message
- ❑ Engage notification / credit services vendor
- ❑ Investigate whether data has been "breached"
- ❑ Determine when notification "clock" started
- ❑ Remediate and protect against future breaches
- ❑ Confirm notification / remediation obligations
- ❑ Determine proper remediation services
- ❑ Assemble contact information for notifications
- ❑ Prepare notification letters, frequently asked questions, and call centers
- ❑ Plan and time notification "drop"
- ❑ Implement public relations strategy
- ❑ Administrative reporting (AGs, HHS, FTC, SEC)
- ❑ Implement Cyber Risk Management Program

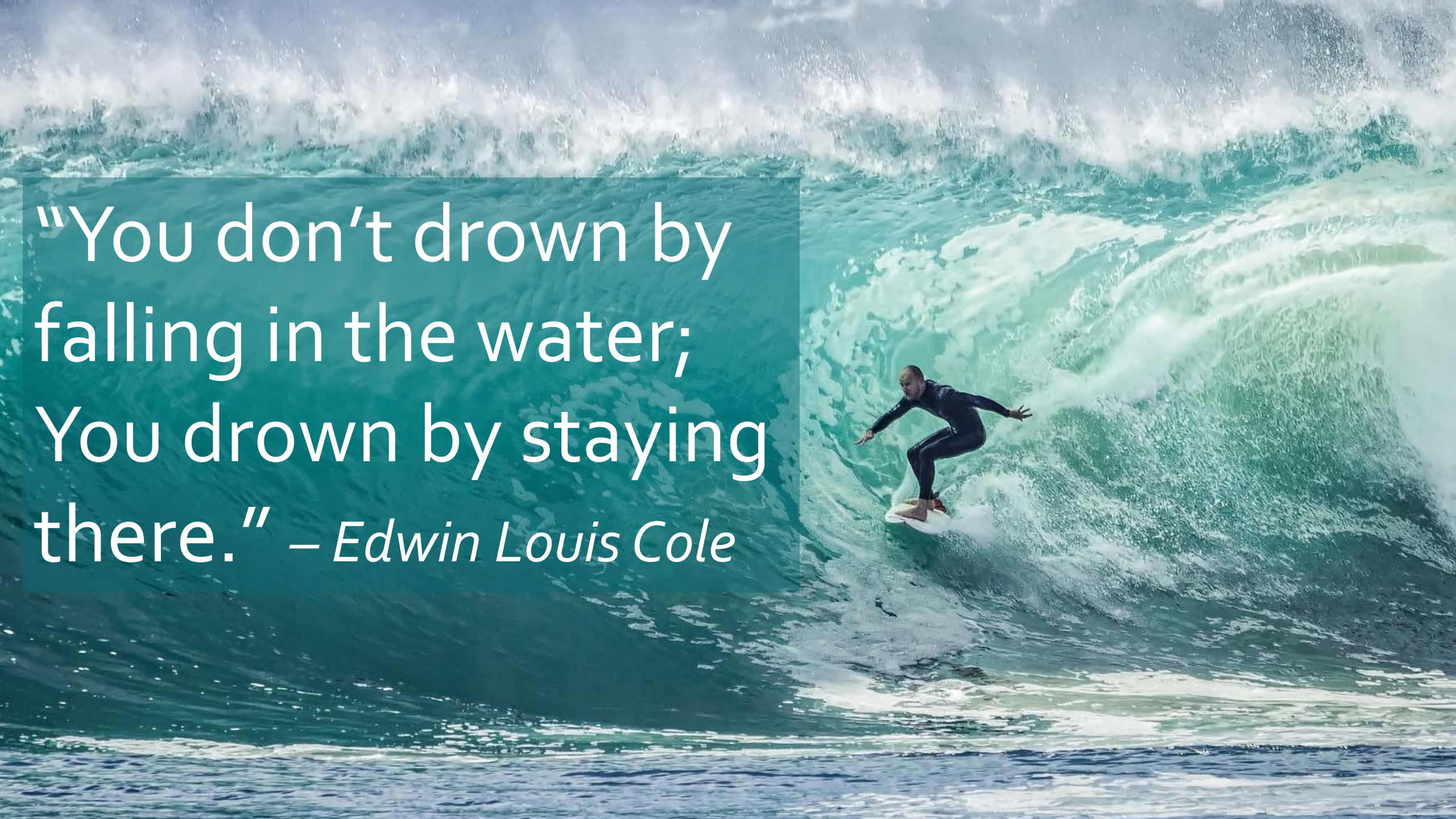
"Target has demonstrated . . . that the work of the Data Breach Task Force was focused not on remediation of the breach . . . but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation that was already pending and was reasonably expected to follow."
In re Target Corp. Customer Data Breach

"Firms must adopt written policies to protect their clients' private information . . . they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."
S.E.C. v. R.T. Jones Capital Equities Mgt.

For more information, please contact:
Shawn E. Tuma
Cybersecurity & Data Privacy Partner
Direct: 214.472.2135 | Mobile: 214.726.2808
shawn.tuma@solidcounsel.com
Blog: www.shawnetuma.com

Scheef & Stone, L.L.P. is a full service business law firm providing clients with litigation, transactional, technology, and intellectual property services with expertise in business cyber risk areas of cybersecurity, data security, data breach, data privacy, and computer fraud.

www.solidcounsel.com


"You don't drown by falling in the water; You drown by staying there." – *Edwin Louis Cole*

- Board of Directors & General Counsel, Cyber Future Foundation
- Board of Advisors, North Texas Cyber Forensics Lab
- Policy Council, National Technology Security Coalition
- Cybersecurity Task Force, Intelligent Transportation Society of America
- Practitioner Editor, Bloomberg BNA – Texas Cybersecurity & Data Privacy Law
- Cybersecurity & Data Privacy Law Trailblazers, National Law Journal (2016)
- SuperLawyers Top 100 Lawyers in Dallas (2016)
- SuperLawyers 2015-17
- Best Lawyers in Dallas 2014-17, D Magazine (Cybersecurity Law)
- Council, Computer & Technology Section, State Bar of Texas
- Privacy and Data Security Committee of the State Bar of Texas
- College of the State Bar of Texas
- Board of Directors, Collin County Bench Bar Conference
- Past Chair, Civil Litigation & Appellate Section, Collin County Bar Association
- Information Security Committee of the Section on Science & Technology Committee of the American Bar Association
- North Texas Crime Commission, Cybercrime Committee & Infragard (FBI)
- International Association of Privacy Professionals (IAPP)

Shawn Tuma
Cybersecurity Partner
Scheef & Stone, L.L.P.
214.472.2135
shawn.tuma@solidcounsel.com
@shawnetuma
blog: www.shawnetuma.com
web: www.solidcounsel.com

SCHEEF & STONE
SOLID COUNSEL