

- 9:30 – 10:00 a.m.** Registration
- 10:00 – 10:15 a.m.** Welcome and Introduction  
*James E. O'Connor*  
*Vickie B. Ahlers*
- 10:15 – 11:00 a.m. Getting to Accountability: Investing in Your Data Security Program**  
From the board of directors down to the last employee, your organization must understand and approach cybersecurity as an enterprise-wide risk management issue. It is imperative that cyber security preparedness not be relegated only to the IT department. This session will discuss the critical steps in establishing and investing in a data security and incident response program, including board accountability and oversight, that helps position companies to avoid, be prepared for and respond to data privacy or security incidents.  
*James E. O'Connor*  
*Stephanie A. Mattoon*
- 11:00 – 11:45 a.m. "Help! We've Been Hacked!" A Step-by-Step approach to Responding to a Breach**  
In today's cyber world, we are constantly one step behind the hackers. Knowing how to respond when your company has been the victim of a hack or other privacy or security incident is imperative. This session takes participants through the steps of responding to a breach, from engaging the appropriate vendors, to customer or employee notifications, to maintaining the right documentation to respond to regulator inquiries.  
*Vickie B. Ahlers*  
*Michael W. Chase*  
*AriAnna C. Goldstein*  
*Chris Worley, Senior Consultant, Continuum Security Solutions*
- 11:45 a.m. – 1:00 p.m. Lunch & Presentation: The Coming of Age of the Internet of Things–What's on the Horizon?**  
*Professor Justin (Gus) Hurwitz, Nebraska College of Law*  
*Moderated by James E. O'Connor and Y. Kamaal Patterson*
- 1:00 – 2:00 p.m. State of the Cyber Market: Considerations, Coverage and Trends**  
Whether and how to manage cyber risks through insurance is one of the most frequent questions being discussed in board rooms today. This session brings together an expert panel of insurance brokers to discuss key insurance issues, such as how to compare cyber policies, the benefits of building a cyber tower, anticipated increases in cyber coverage rates, and what "gotchas" may be hidden in cyber policies that affect coverage.  
*John Marshall, SilverStone Group*  
*Andy Sibbersen, Harry A. Koch*  
*Miles Weis, Holmes Murphy*  
*Moderated by James E. O'Connor*
- 2:00 – 2:30 p.m. Post-Breach–What to Expect from a Regulatory Investigation and the Threat of Litigation**  
Before you've even confirmed what happened involving a data privacy or security incident and notified the affected individuals, a lawsuit likely has been filed and the attorney general or another regulatory agency is asking questions. What should you do? This session discusses what we can learn from the growing cyber litigation landscape and key steps in responding to a regulatory investigation.  
*Vickie B. Ahlers*  
*Jill Robb Ackerman*

**2:30 – 2:45 p.m.** Break and Refreshments

**2:45 – 3:45 p.m. Saving Your Reputation in the Court of Public Opinion: The Public Relations Perspective**

Think armchair quarterbacking is just for football? Ask the CEO of a company that has been the target and see what he or she thinks. Everyone seemingly has an opinion on how well a company victimized by a cyber attack handled the incident from a public relations perspective. In this session, a panel of experts in crisis communications and public relations will share their experiences in how best to save your reputation following a cyber event.

*Doug Parrot and Mary Palu, Bailey Lauerman  
Lauri Freking, Wixted & Co.  
Marcia Austin, Hill+Knowlton Strategies  
Moderated by Jill Robb Ackerman*

**3:45 – 4:45 p.m. The Regulatory and Enforcement Landscape: Insight from the Insiders**

*This session will feature representatives from federal and state governmental agencies, law enforcement and prosecutors who have experience in dealing with cybercrimes and data protection issues. The panel will highlight current areas of focus, provide regulatory and enforcement insights and an update on where governmental agencies are heading with cyber security, data privacy and critical infrastructure protection. It will also provide best practices on how to work with governmental agencies, law enforcement and regulators.*

*Special Agent James Craig, FBI  
Dan Birdsall, Assistant Attorney General, State of Nebraska  
Deborah Gilg, U.S. Attorney, District of Nebraska  
Greg Hollingsead, Protective Security Advisor, Department of Homeland Security  
Moderated by James E. O'Connor and Vickie B. Ahlers*

**4:45 p.m. Closing Remarks**

*Please join us in the hotel lobby bar for complimentary cocktails and appetizers immediately following the presentation.*

# TECHNOLOGY & DATA PROTECTION FORUM

## Getting to Accountability: Investing in Your Data Security Program

*James E. O'Connor*

*Stephanie A. Mattoon*

## Getting to Accountability: Investing in Your Data Security Program



James E. O'Connor  
Stephanie A. Mattoon

---

---

---

---

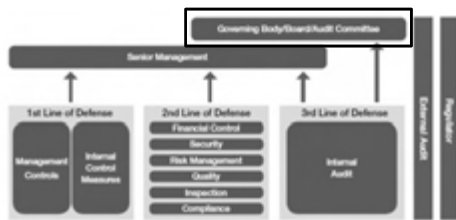
---

---

---

---

## Three Lines of Defense



From the *Institute of Internal Auditors Research Foundation 2014 Report*

---

---

---

---

---

---

---

---

## Agenda

- Board's governance role
- D&O lawsuits
- Lessons learned
- Guiding principles for the Board
- What should the Board ask?
- What should you tell the Board?
- Summary/Q&A

---

---

---

---

---

---

---

---

## Recent High-Profile Attacks



---

---

---

---

---

---

---

---

## Business Implications

- Intellectual Property Theft
- Business Interruption
- Reputational Damage
- Regulatory Actions
- Litigation
  - Now → shareholder lawsuits *against directors and officers*

---

---

---

---

---

---

---

---

## Board's Governance Role

- State law – D&O fiduciary duties:
  - Loyalty
  - Due care
- Board's oversight of risk management:
  - Inform itself on nature and extent of risk
  - Ensure company has controls in place
  - Monitor those controls
- Officers implement risk controls

---

---

---

---

---

---

---

---

### Heartland Financial Lawsuit (2008 breach)

- Securities fraud claim against CEO and CFO
- 10-K: Heartland "places significant emphasis on maintaining high level of security" and maintains network that "provides multiple layers of security to isolate its databases from unauthorized access"
- Court → fact of breach does not necessarily mean statements were false
  - Company invested significant money in data security and did place high emphasis on security, but systems were nevertheless overcome

---

---

---

---

---

---

---

---

### Target Lawsuit (2013 breach)

- Officers and directors breached fiduciary duties by:
  - "Failing to implement a system of internal controls to protect customers' personal and financial information"
  - "Causing or allowing the Company to conceal the full scope of the data breach"
  - Audit committee "completely and utterly failed in their duty of oversight"

---

---

---

---

---

---

---

---

### Wyndham Lawsuit (2008-2010 breaches)

- Court dismissed shareholder derivative lawsuit → plaintiff failed to allege facts showing bad faith or unreasonable investigation:
  - Board discussed the cyber-attacks at 14 meetings
  - GC gave data security presentation at each meeting
  - Audit Committee discussed breaches at 16 meetings
  - Company had retained third-party tech firm to investigate each breach and recommend enhancements

---

---

---

---

---

---

---

---

## Home Depot Lawsuit (2014 breach)

- Board aware company was vulnerable to data breach
  - SEC filings identified security breach as “Risk Factor”;
  - CEO acknowledged systems were “desperately out of date”
  - Remedies were in process
- “Complacent” by failing to implement protective measures in timely manner
- Violation of Payment Card Industry Data Security Standards
- Several high-profile data breaches at other major retailers (Target, Neiman Marcus) alerted Board to a “heightened probability that Home Depot would also be attacked”

---

---

---

---

---

---

---

---

## Lessons Learned

- Make data security regular topic at Board meetings
- Designate Board committee with primary oversight
- Periodically retain third party consultants to assess data protection systems (and recommend improvements)
- Document steps taken to remedy deficiencies
- Demonstrate that Company takes data protection seriously – commitment of money and HR

---

---

---

---

---

---

---

---

## Changing Landscape

- Investor reaction – are data breaches still viewed as “random,” CODB?
- Cybersecurity is now expected
- Attack/breach is indication of deficiency, violation of duties
- Failure to prepare for attack → answer to shareholders (and SEC...)

---

---

---

---

---

---

---

---

## SEC Cyber Security Guidance

- Corporation Finance Guidance – October 13, 2011
- Cyber Security Roundtable – March 26, 2014
- Investment Management Update – April 2015

---

---

---

---

---

---

---

---

## SEC Cyber Security Guidance

- Disclosure if cyber-risks “are among the most significant factors that make an investment in the company speculative or risky”

---

---

---

---

---

---

---

---

## Regulators in the Financial Services Industry

- Third-party risks are not adequately addressed
- Risk management
- Federal Financial Institutions Examination Council (FFIEC)- cyber security assessment tool
- New York State Department of Financial Services



---

---

---

---

---

---

---

---



### PWC 2015 Survey

- 87% of US chief executives worried cyber threats could impact growth prospects
- Up from 69% the year before
- A record 79% of survey respondents detected a security incident in the past 12 months

---

---

---

---

---

---

---

---

### Organizational Roles:

- Chief Information Security Officer-CISO
- Chief Security Officer-CSO
- Chief Privacy Officer-CPO
- Chief Risk Officer-CRO
- Chief Information Officer-CIO

---

---

---

---

---

---

---

---

### Chief Information Security Officer

- Debate about how to integrate the security function into the organizational structure
- Report to the CIO, CEO, CFO, COO, and the Board

---

---

---

---

---

---

---

---

## Cyber Security is a Board Issue

- Impact of cyber security is systemic
- Financial impact can be significant
- Compliance becoming more challenging and increasingly costly



---

---

---

---

---

---

---

---

## Cyber Security is a Board Issue

- Internet of Things - compromise can cause extreme risks and tremendous physical damage
- Cyber security insurance should be considered as a regulatory hedge against cyber-risks
- Cyber attacks can result in substantial financial losses and damage brand reputation

---

---

---

---

---

---

---

---

Board engagement in cyber-risks



---

---

---

---

---

---

---

---

## Board Reporting

- Risk Committee
- Audit Committee
- Finance Committee
- Executive Committee
- Full Board

---

---

---

---

---

---

---

---

## Guiding Principles for the Board

- Approach cyber security as an enterprise-wide risk
- Understand legal implications of cyber-risks
- Set expectations with adequate resources
- Focus on risks to avoid, accept, mitigate or transfer

From the *Institute of Internal Auditors Research Foundation 2014 Report*

---

---

---

---

---

---

---

---

## Questions the Board Should Ask:

- Does the entity use a security framework?
- What are the top cyber-risks?
- How are employees trained?
- What were the results of the last cyber assessment?

---

---

---

---

---

---

---

---

## Questions the Board Should Ask:

- What is the cyber-risk budget?
- How is cyber security governance managed?
- Provide a copy of the cyber incident response plan

---

---

---

---

---

---

---

---

## Security Budget

- Budget reflects corporate priority
- Budgeting is often complex undertaking
- Many ways to set a budget
  - Senior management
  - Zero-based assessment of risks
  - “Feels right”
  - Percentage of overall IT budget

---

---

---

---

---

---

---

---

## Security Budget

Percent of IT Budget	Respondents
< 1%	9%
1% - 2%	25%
3% - 5%	31%
6% - 10%	10%
11% - 15%	8%
16% - 20%	6%
Over 20%	11%

*Poneman 2015 Global Study on IT Spending & Investments*

---

---

---

---

---

---

---

---

## What Should You Discuss with the Board?

- Responsibilities
- Cyber security policies and procedures
- Budget for cyber security
- Data mapping
- Cyber insurance



"I'd like to begin by making the same point about twenty times in a row."

---

---

---

---

---

---

---

---

## What Should You Discuss with the Board?

- Selection of experts (forensic, breach & legal)
- Third-party cyber due diligence
- Physical security
- Assessment results (at least annual)
- Lessons learned

---

---

---

---

---

---

---

---

## Three Lines of Defense



From the Institute of Internal Auditors Research Foundation 2014 Report

---

---

---

---

---

---

---

---

## Summary

- Cyber security should be a priority issue
- Directors:
  - Do not have to be experts
  - May rely on information and advice



---

---

---

---

---

---

---

---

## Summary

- Board should:
  - Inform itself regarding cyber security risk
  - Understand company's risk profile
  - Ensure that proper resources are available
  - Monitor controls

---

---

---

---

---

---

---

---

## Summary

- Review cyber security reporting
  - Content
    - Incident readiness and response
    - Threat intelligence
    - Cyber security governance
    - Assessments
  - Board recipients
  - Who prepares and delivers
- Review Board minutes

---

---

---

---

---

---

---

---

Questions?

---

---

---

---

---

---

---

---

Thank You

James E. O'Connor  
(402) 636-8332 | joconnor@bairdholm.com

Stephanie A. Mattoon  
(402) 636-8238 | smattoon@bairdholm.com

---

---

---

---

---

---

---

---

# TECHNOLOGY & DATA PROTECTION FORUM

## **“Help! We’ve Been Hacked!” A Step-by-Step Approach to Responding to a Breach**

*Vickie B. Ahlers*

*Michael W. Chase*

*AriAnna C. Goldstein*

*Chris Worley*

*Senior Consultant, Continuum Security Solutions*



**Chris Worley**

Senior Consultant, Continuum Security Solutions  
[chris.worley@cwsecurity.com](mailto:chris.worley@cwsecurity.com) | (402) 916-1836

---

Chris Worley is a Senior Consultant for Continuum Security Solutions. He has over ten years of experience in consulting, network support, and information security positions at companies across a variety of industries. Chris specializes in several domains of information security including penetration testing, enterprise vulnerability and patch management, hardening operating systems, certification and accreditation, compliance auditing, and developing and maintaining business continuity and disaster recovery plans.

Chris holds a Masters Degree in MIS with an emphasis in Information Assurance from the Peter Kiewit Institute at the University of Nebraska-Omaha. In addition, he holds several professional certifications including the Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), GIAC Security Essentials Certification (GSEC), GIAC Systems and Network Auditor (GSNA), GIAC Certified Enterprise Defender (GCED), GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), GIAC Certified Intrusion Analyst (GCIA), Payment Card Industry Data Security Standard Qualified Security Assessor (PCI-DSS QSA) certifications, and has received training in Advanced Penetration Testing.

Help! We've Been Hacked!  
A Step-by-Step Approach to  
Responding to a Breach

Vickie B. Ahlers  
Michael W. Chase  
AriAnna C. Goldstein  
Chris Worley, Continuum Security Solutions

---

---

---

---

---

---

---

---

"No matter how much is spent or  
done, we are not  
immune from attack."

Anthem statement to NAIC Cybersecurity Task Force

---

---

---

---

---

---

---

---

Responding to an Incident

Session will discuss:

- Incident Response Plan
- Forensic Investigation
- Customer/Employee Notification and Related Issues

---

---

---

---

---

---

---

---

### Why Rapid Response is Critical

- Containment of incident/eradication of attackers to prevent critical data from being exposed (or further exposure)
- Collect and preserve forensic evidence
- Accurate assessment of precisely what happened

---

---

---

---

---

---

---

---

### Why Rapid Response is Critical

- Communicate accurate information to affected individuals and media in appropriate timeframe
  - Balance notification with securing network
- Remediate the problem
- Minimize reputational harm
- Reduce financial exposure

---

---

---

---

---

---

---

---

### Incident Response Plan: Activation

- Activating Your Incident Response Plan (IRP)
  - Many actions occurring simultaneously in IRP
  - Who do you call first?
    - CISO?
    - Legal Counsel?
    - Broker/Insurer?
- Engage legal counsel to invoke attorney-client privilege over engagement of other vendors and documentation
- According to DOJ's recent guidance, companies should ensure legal counsel is experienced in cyber incident management to reduce response time during an incident

---

---

---

---

---

---

---

---

## Incident Response Plan: Activation

- Activation and incident response activities: Calls/In-person vs. Emails
  - Many "facts" in the beginning will turn out not to be accurate
  - Don't leave a paper trail of assumptions or speculation
  - Don't tip off attackers – if attack is active, take steps not to let attackers know they are detected
- Activation for non-electronic incidents
  - Mistake: Many IRPs only cover computer or electronic incidents
  - Don't overlook other types of information compromise and understand how you will respond (significant percentage of breaches are of paper records)

---

---

---

---

---

---

---

---

## Incident Response Plan: Assembling the Team

- Assembling your Incident Response Team
  - Everyone should know his or her role and first steps
  - Who is in charge of maintaining official documentation of all aspects of response?
    - Timeline of events
    - Detailed record of calls, meetings, etc.
    - If in-house legal counsel does not keep official documentation, should be prepared for legal counsel
    - Incident report to assume regulatory investigation – support defense positions taken
  - Meetings: conference calls or in-person meetings to update information on set schedule (hourly?, daily?)

---

---

---

---

---

---

---

---

## Incident Response Plan: Vendors

- Immediately engage (or activate if already on retainer) critical vendors
- If insured, do you know which vendors your insurance company will approve?
  - Negotiate in advance of selecting insurer (if possible)
  - Negotiate in advance of incident at very least
- Establish relationships in advance and share your IRP with those vendors

---

---

---

---

---

---

---

---

### Incident Response Plan: Assessment

- Accurate assessment of incident to calibrate response
  - Categorize data and exposure (did they get to the crown jewels?)
  - Origin of intrusion
  - Any other victim organizations
- Initial assessment will dictate whether law enforcement is contacted
- Assessment will determine what level of notification is required (if any) and when

---

---

---

---

---

---

---

---

### Incident Response Plan: Containment and Remediation

- Efforts/ability to eradicate the problem affected by whether incident was self-detected and how long from intrusion to detection
  - Average around 12 months
  - Early detection with prompt eradication can significantly reduce exposure
- If intrusion is ongoing, who has authority to power down critical systems?
- Restoring public-facing system critical to both business continuity/operations and public perception

---

---

---

---

---

---

---

---

### Incident Response Plan: Remediation

- Don't focus remediation efforts inward only
- Sony: Amended class action filed by employees in March 2015:
  - Sony Pictures Entertainment has "focused on its own remediation efforts, not on protecting employees' sensitive records or minimizing the harm to its employees and their families."

---

---

---

---

---

---

---

---

## Incident Response Plan: The Vendor Breach

- Does your IRP address how you will respond to a breach by a vendor?
- Vendors still significant source of data compromise
- Discuss response logistics with key vendors in advance – include as part of contract negotiations
  - e.g., how quickly must they notify you of a breach
  - Regularly done in health care industry but not always in other industry vendor relationships

---

---

---

---

---

---

---

---

## Agenda

- What steps to take during and after a breach or an incident?
- Incident Response vs. Forensics
- What can I do vs. Leave it to the experts
- Common failures

---

---

---

---

---

---

---

---

## Preparation and Response

- Business Impact Analysis
  - Identify risks, identify assets, define importance
- Identify and Engage Local Experts
  - who can help, response time, SLA's
- Technical Controls
  - What will I need during and after a breach
- Educate
  - What “to do” and “not to do”

---

---

---

---

---

---

---

---

## 6 Steps of Incident Response

- Preparation
- Identification
- **Containment**
- **Eradication**
- Recovery
- Lessons Learned

---

---

---

---

---

---

---

---

## Step 1 - Preparation

- Identify Risks (**BIA, Risk Assessments**)
- Identify Response Team - **Identify and Engage Experts (Retainer, SLA's)**
- Technical and Administrative Controls
  - Having **logging** in place on critical assets, entry and exit points, and at key locations and maintain the logs for at least 90 days, ideally longer. Many breaches are not discovered until much later.

---

---

---

---

---

---

---

---

## Step 2 - Identification

- **Initial Identification – normal vs. abnormal**
- **Initiate documentation of event – time, date, resource, etc. (manual or automated)**
- **Define Action – observe or react, ongoing or past event (Log review)**
- Decision to elevate or involve IR Team
- Depending on severity – Isolation of target

---

---

---

---

---

---

---

---

### Step 3 - Containment

- Identify the events impact and reach
  - Where is this taking place?
    - External device or internal database with sensitive information?
  - What is the potential impact
    - Secondary event? Trojan Horse or diversion
    - Has data left the environment? How?
    - Was the attacker able to hide their tracks
  - Internal versus External
    - Where did the attack originate

---

---

---

---

---

---

---

---

### Step 3 - Containment

- Is immediate action required? If so what –
  - Stop the action – a technical response
    - Block the attacker?
  - Isolate the system to maintain the evidence for forensics review and potential legal actions
  - Call in the Calvary (Continuum, Law Enforcement, etc...)

---

---

---

---

---

---

---

---

### Step 4 - Eradication

- Identify root cause
- Vulnerability Analysis
- Address the issues
  - Remove malware, patch or upgrade systems or applications, firewall or IDS/IPS rules, improve defenses or processes
- Have we taken the required steps to prevent a reoccurrence?

---

---

---

---

---

---

---

---



### Step 5 & 6 – Recovery & Learned

- Clean or rebuild the systems or applications
- Restore Operations & Monitor (Logging)
- Discuss lessons learned with team members and engaged experts
- Update documents to reflect lessons learned

---

---

---

---

---

---

---

---

### Dig Up the Bones - Forensics

- After the event is over or under control, you may want or need to engage a CFE.
  - Lessons learned
  - Compliance or insurance requirements
  - Identify the parties or systems involved
  - Understand the full impact, what was exposed, did data leave the network
  - Legal recourse

---

---

---

---

---

---

---

---

### Don't Do That! Limit the Damage

- Avoid Contamination of the Crime Scene
  - Do not power off, restart or reboot the systems, avoid logging on with other accounts
  - Evaluate before acting
    - Running malware or AV scan could change the properties of the files – could impact legal recourse
    - Limit the amount of changes to the system
    - Maintain the normal state of the system of possible
- Engage the experts
  - Can be internal if appropriately trained

---

---

---

---

---

---

---

---

## What Should I Do?

- Engage the experts as early as possible
- Have sufficient logs in place
  - minimum of 90 days of critical assets and connected to devices, firewalls, etc.
- Maintain good backups – Golden Image
  - Can do comparisons to see what's changed
- Isolate from the network if needed ( do not power off)

---

---

---

---

---

---

---

---

## Common Failures

- Not knowing who to contact and when
  - Engaging experts sooner may help limit exposure and preserve evidence
- Identify key assets and monitor them
  - Insufficient logging is a major issue – discovery of event often occurs months after the fact
    - Logs are often overwritten and not stored securely
    - Log different layers of the network (External and Internal)
    - Investigators can't follow the trail or identify exposures
- Restrict what leaves your network and where it can go
  - If you don't do business in China, why is your data going there?
- Know your pain tolerance
  - How much downtime is acceptable
    - Should I leave a compromised system running?
  - At what point in time are business operations impacted

---

---

---

---

---

---

---

---

## Breach Notification

### Questions to Ask

- What types of information?
- Where did the breach occur? (Vendor or business associate?)
- How many affected individuals?
- Do you have current addresses?

---

---

---

---

---

---

---

---

## Breach Notification

### Questions to Ask

- Who will draft notification letters?
- Some organizations engage a third party to notify (AllClear ID; Kroll)
- Organization should review letters and propose changes

---

---

---

---

---

---

---

---

## State Law Patchwork

- All but 3 states have some form of data breach laws
- 8 states are enacting second generation laws



---

---

---

---

---

---

---

---

## State Law Patchwork

- Statutory vs. "Suggested" Notifications
- HIPAA considerations

---

---

---

---

---

---

---

---

## Second Generation Data Breach Laws

- Attorney General Notification
- More expansive definition of "Personal Information"

---

---

---

---

---

---

---

---

## Second Generation Data Breach Laws

- Notification Timeline
- Mandated credit monitoring



---

---

---

---

---

---

---

---

## Second Generation Data Breach Laws

- California
  - Clarification of acceptable encryption
  - Format of notification letters
    - What happened?
    - What information was involved?
    - What are we doing?
    - What can you do?
    - For more information

---

---

---

---

---

---

---

---

## Additional Considerations

- Identity theft protection
- Informing consumers
- Call center
- Website information



---

---

---

---

---

---

---

---

## Breach Notification

Other Considerations

- Recent poll: 62% of consumers have received at least 2 DBN letters
- Many individuals do not understand contents of the letters
  - Connection to the affected organization (i.e. Wellmark/Anthem)

---

---

---

---

---

---

---

---

## Breach Notification

Other Considerations

- Ponemon Institute: 32% of consumers do nothing
- Anthem: 79 million individuals; **4%** accepted free ID theft coverage
- Premera: 10.5 million individuals; **7.4%** accepted free ID theft coverage

---

---

---

---

---

---

---

---

**Breach Notification**  
Other Considerations

- Some consumers might have “breach fatigue”
  - Breach overload – Sony, Target, Home Depot, Dairy Queen, etc., etc., etc.,
- Some consumers are worried about giving more personal information to credit monitoring companies (i.e., social security number)

---

---

---

---

---

---

---

---

**Breach Notification**  
Other Considerations

- Consider an additional explanatory communication
- Document returned/undeliverable letters
  - Substitute notice requirements
  - HIPAA: if >10, website posting and toll-free number

---

---

---

---

---

---

---

---

**Thank You**

Vickie Ahlers 402.636.8230 vahlers@bairdholm.com	Michael Chase 402.636.8326 mchase@bairdholm.com
AriAnna Goldstein 402.636.8236 agoldstein@bairdholm.com	Chris Worley 402.916.1836 chris.worley@cwsecurity.com

---

---

---

---

---

---

---

---

# TECHNOLOGY & DATA PROTECTION FORUM

## The Coming of Age of the Internet of Things—What's on the Horizon?

*Professor Justin (Gus) Hurwitz*

*Nebraska College of Law*

*Moderated by  
Y. Kamaal Patterson*

## Notes

---



## **Justin (Gus) Hurwitz**

Assistant Professor of Law, University of Nebraska College of Law

[ghurwitz@unl.edu](mailto:ghurwitz@unl.edu) | (402) 472-1255

---

Professor Justin (Gus) Hurwitz joined the College of Law faculty in 2013. His work builds on his background in law, technology, and economics to consider the interface between law and technology and the role of regulation in high-tech industries. He has a particular expertise in telecommunications law and technology.

Professor Hurwitz previously was the inaugural Research Fellow at the University of Pennsylvania Law School's Center for Technology, Innovation and competition (CTIC), prior to which he was a Visiting Assistant Professor at George Mason University Law School. From 2007–2010 he was a Trial Attorney with the United States Department of Justice Antitrust Division in the Telecommunications and Media Enforcement Section.

Professor Hurwitz has a background in technology having worked at Los Alamos National Lab and interned at the Naval Research Lab prior to law school. During this time his work was recognized by organizations such as the Federal laboratory Consortium, R&D Magazine, Los Alamos National Lab, IEEE & ACM, and the Corporation for Education Network Initiatives in California. In addition, he held an Internet2 Land Speed World Record with the Guinness Book of World Records.

Professor Hurwitz received his JD from the University of Chicago Law School, where he was an articles editor on the *Chicago Journal of International Law* and received Olin and MVP2 law and economics scholarships. He also holds an MA in Economics from George Mason University. He received his BA from St. John's College.

# TECHNOLOGY & DATA PROTECTION FORUM

## State of the Cyber Market: Considerations, Coverage & Trends

*John Marshall*  
*SilverStone Group*

*Andy Sibbernsen*  
*Harry A. Koch*

*Miles Weis*  
*Holmes Murphy*

*Moderated by*  
*James E. O'Connor*

## Notes

---

## **John Marshall**

Principal & Shareholder, Healthcare Risk Services Division, SilverStone Group

[jmarshall@ssgi.com](mailto:jmarshall@ssgi.com) | (402) 964-5559

---

John has lived and breathed healthcare from a very young age. Growing up in a family who works in the industry, he knows the challenges and rewards first-hand. His entrepreneurial drive has been with him since childhood. He and his younger brothers had a lawn business for many years and, at one time, had Gary Hurley (retired CEO of SilverStone Group) as a customer. When John's resume landed on his desk a few years later, Gary remembered how John always did an outstanding job and decided to give him a chance at SilverStone Group.

Currently, John serves as the head of the Healthcare Risk Services division for SilverStone Group, in addition to handling all educational institution clients for the firm. John's team works with Associates throughout SilverStone Group to develop strategies to reduce the total cost of risk for clients firm-wide. Throughout his career, John has developed an expertise in medical malpractice insurance and risk management. He has also developed a proprietary risk identification process at SilverStone Group that helps healthcare and educational organizations control business risk.

Working at SilverStone Group allows John to be on the leading edge of industry offerings. With the help of his team, he is able to create, offer and implement solutions to the challenges that others say can't be overcome. John is able to quantify the exposures his clients have faced in the past, giving his team the ability to prioritize, and hopefully prevent, those same problems happening to new and current clients.

John is a frequent contributor to local trade journals and serves as a public speaker at several healthcare associations each year, providing unique data on risk management and medical malpractice market conditions. His articles on the subject of medical malpractice and risk management have been featured in our own SilverLink magazine as well as national publications such as Medical Economics.

He has previously served two-year terms as board chairman of VODEC and the Southwest Iowa Red Cross Chapter. In 2005, John was honored as one of the top 40 business professionals under the age of 40 by the Midlands Business Journal, an Omaha publication.

John and his wife, Andrea, have worked with several philanthropic organizations in the area, helping with fundraising, strategic development and financial accounting. Andrea also serves on both the summer arts festival and MerryMakers' boards. The couple likes living in downtown Omaha, experiencing the "urban life." Together they enjoy traveling, hiking adventures, scuba diving and running outdoors.

# TECHNOLOGY & DATA PROTECTION FORUM

## Post-Breach—What to Expect from a Regulatory Investigation and the Threat of Litigation

*Jill Robb Ackerman*

*Vickie B. Ahlers*

Post Breach – What to Expect from a  
Regulatory Investigation and the  
Threat of Litigation

Jill Robb Ackerman  
Vickie Ahlers

---

---

---

---

---

---

---

---

Regulatory Investigations and  
Enforcement

- Regulatory involvement post-breach at an all-time high
- Many view the potential for regulatory fines and monitoring and cost of regulatory defense as most significant risk

---

---

---

---

---

---

---

---

Regulatory Investigations and  
Enforcement

- Multiple state and federal agencies can/will investigate same incident
  - **Office for Civil Rights**
    - Covered entities and business associates under HIPAA
    - Automatic if over 500 affected; “willful neglect”
    - Settlements ranging from \$375k - \$4M
    - Large and small entities
    - Public and private

---

---

---

---

---

---

---

---

## Regulatory Investigations and Enforcement

- Multiple state and federal agencies can/will investigate same incident
  - **Federal Trade Commission**
    - “unfair” or “deceptive” trade practices
    - From 2002 – 2014, 50 cases brought by FTC
    - Internet giants such as MySpace, Facebook, Google, Snapchat, LifeLock
    - More recently targeting smaller companies
    - Have successfully defended challenge to authority to regulate
    - Multi-million dollar fines; 20 year monitoring

---

---

---

---

---

---

---

---

## Regulatory Investigations and Enforcement

- **State Attorney Generals**
  - State consumer protection laws
  - HITECH gave State AGs authority to enforce HIPAA
- **FCC**
  - Recent significant fines (\$25 million settlement with AT&T on 4/8/15)
  - “We’ve only begun to exercise” power in this area

---

---

---

---

---

---

---

---

## What Regulators Ask For

- Detailed description of incident including when it occurred, how long it occurred, how access to personal information was obtained and date of discovery
- Whether investigation was conducted and a summary/report of investigation
- Copies of all “documents gathered during and related to the investigation as well as a copy of your findings”

---

---

---

---

---

---

---

---



## What Regulators Ask For

- Documentation supporting any claims that your company/facility responded to the incident(s) and mitigated, to the extent practical, the harmful effects of the incident.
- Provide any safeguards, protections, encryption, or other mechanisms to limit access to consumers' personal information that company had in place prior to the breach
- Indicate what steps were taken to restore integrity to the computerized data system and when those remedial steps were taken.

---

---

---

---

---

---

---

---

## What Regulators Ask For

- Copies of privacy and security policies and procedures – all versions in effect for last six years
- Evidence that policies are deployed and consistently applied (e.g., sanctions policy)
- Copies of risk assessments conducted by organization – all assessments for prior six years
- Risk mitigation plans developed in response to identified risks and evidence of remediation

---

---

---

---

---

---

---

---

## What Regulators Ask For

- Copies of breach notification letters sent to affected individuals
- A list, in electronic format, of all residents of the state affected by the breach, including their names, physical addresses and, if company possesses them, emails.\*
- Proof of date of mailing
- Log of non-deliverable letters
- Vendor/Business Associate agreements in place
- Disaster recovery and business continuity plans

\*NE AG request

---

---

---

---

---

---

---

---

### Themes of Investigation

- Did you analyze your risks ahead of time such that this risk should have been known?
- Did you actually know of the risk and for how long?
- What had you done in advance to protect data from the risk?

---

---

---

---

---

---

---

---

### Themes of Investigation

- Were employees adequately trained?
- Once you detected the compromise, how quickly did you react to stop the problem and inform affected individuals?
- If employee malfeasance caused the problem, did you sanction appropriately?
- Did you meet all statutory/regulatory requirements in the process?

---

---

---

---

---

---

---

---

### Investigation Considerations

- Should you disclose prior security risk assessments highlighting risk areas (may or may not have been exploited in current breach)
- Should you waive the attorney client privilege in connection with the investigation?

---

---

---

---

---

---

---

---

## Cyber Breach LAWSUITS ARE BIG BUSINESS – For Crooks

and for Lawyers, Regulators, Experts, E-Discovery Vendors, Insurance Companies.....



and a big drain on business: healthcare \$398 v. financial \$259 v. \$217 average cost per record

---

---

---

---

---

---

---

---

## Who Might Sue You?

- Class actions by the folks whose data was stolen
- Your Shareholders or Partners
- Your Bank or Credit Card Processor
- Your Creditors when your company is in financial ruin

---

---

---

---

---

---

---

---

## Recurring Themes in Lawsuits

- *Previously warned of vulnerabilities in system*
  - *Audits - Awareness of other lawsuits*
- *Knew the system would be a target*
- *Failed to implement recommendations from audit*
- *Failed to test system*
- *Knew of alternatives to make site more secure*
- *Breached contractual obligations*
- *Breached representations*
- *Negligence*
- *Unjust Enrichment*

---

---

---

---

---

---

---

---

## Directors and Officers

- Shareholder Derivative Suits
- **Home Depot** Breach - Northern District of Georgia - "breached fiduciary duties of loyalty, good faith, fair dealing and due care" to take reasonable steps to protect customers' personal and financial data and "waste of corporate assets"
  - Breach 9/2014
  - 44 civil actions
  - State and federal investigations
  - Recover costs company incurred as a result of the breach, corporate governance reforms and restitution of compensation and benefits the individual defendants received

---

---

---

---

---

---

---

---

## Options When Sued

- Fight - try to have case dismissed on legal theories
  - Still expensive - Plaintiffs suing on privacy issue have had trouble showing injury
- Settlement
  - Still expensive - **Sony Breach**
    - 50,000 employees affected - Settlement worth up to \$8 million

---

---

---

---

---

---

---

---

## Advocate Medical Group Case Dismissed

- Court determined the damages were too speculative to confer standing
- 4 unencrypted laptops stolen (no evidence stolen for the data)
- Court Rejected Fair Credit Reporting Act Violation

---

---

---

---

---

---

---

---

## AvMed Case Settled

- 2013 awarded \$30 to each about 460,000 individuals affected by breach which represents what should have been paid for security
- $\$30 \times 460,000 = \$13,800,000!$

---

---

---

---


---

---

---

---

## Excellus Breach (Lifetime Healthcare)

- 10.5 million individuals data exposed from a cyber-attack beginning on 8/5/2013 and not discovered until 8/5/15 and disclosed on 9/9/15
- Data was encrypted but hackers gained access to controls 
- Breach of contract and negligence case filed in the Western District of New York

---

---

---

---

---

---

---

---

## Ashley Madison

- Avid Life Media targeted by the 'impact team'
- Canadian class action seeking \$577 million –
  - UK laws on data protection may apply depending on where the server is
- Jane Doe sues in St. Louis because \$19 full delete service did not work as represented



---

---

---

---

---

---

---

---

## Collateral Damage – Lost Jobs

- **Target** – CIO Beth, Jacob CEO Gregg Steinhafel (40 million customers and 46% profit loss)
- **Maricopa County Community College Director of District Information Technology** (2.5 million students and employees)
- **Texas State Comptroller's office** (3.2 million Texans info)
- **Utah Department of Health Head** – Medicaid records over 3 days
- **Accretive Health employee** that did not encrypt laptop stolen from rental car
- **Gold Health Systems employee** downloaded a patient report on a USB and lost it
- **Highmark Inc.** fired **mailroom employee** for an error that led to risk assessments of certain patients being sent to wrong people
- **Georgia Hospital** fired the **custodian and a hospital staffer** when an unencrypted desktop computer was thrown out
- **MDF transcription** fired when posted patient data on a vendors website with no password protection

---

---

---

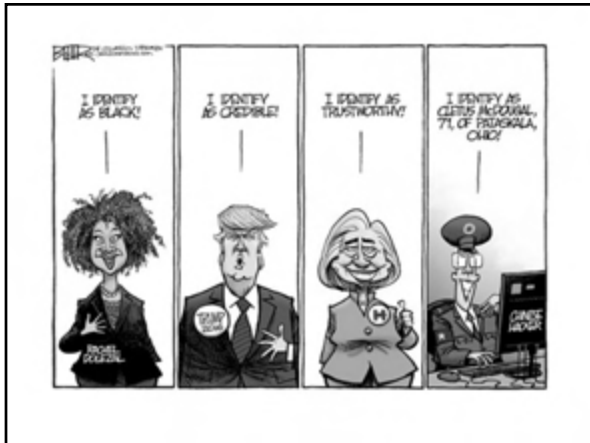
---

---

---

---

---



---

---

---

---

---

---

---

---

Thank You

Jill Robb Ackerman  
402.636.8263  
jackerman@bairdholm.com

Vickie Ahlers  
402.636.8230  
vahlers@bairdholm.com

---

---

---

---

---

---

---

---

# TECHNOLOGY & DATA PROTECTION FORUM

## **Saving Your Reputation in the Court of Public Opinion: The Public Relations Perspective**

*Doug Parrot  
Bailey Lauerman*

*Lauri Freking  
Wixted & Co.*

*Marcia Austin  
Hill+Knowlton Strategies*

*Moderated by  
Jill Robb Ackerman*

## Notes

---



**Doug Parrott**

Executive Vice President of Public Relations, Bailey Lauerma  
(402) 514-9400

---

Doug Parrott started his career as a reporter, and later news executive at KETV, Omaha. He then served as communications director to Nebraska Governor Kay Orr. For the past 25 years he has been a leader in public relations and is the only three-time winner of the Public Relations Society of America Professional of the Year in Nebraska. He recently retired as General Manager and Executive Vice President of Bailey Lauerma and remains a PR consultant to the agency. He also is supervising communications for the 2016 US Olympic Swim Trials.

## Lauri Freking

Senior Trainer & Consultant, Wixted & Company

[lfreking@thinkwixted.com](mailto:lfreking@thinkwixted.com) | (515) 226-0818

---

Lauri combines her wealth of training experience with her journalism background to provide fresh perspectives and customized training for executives in the energy, electric utility, manufacturing, healthcare and retail industries.

A native of Bancroft, Iowa, Lauri has 11 years of experience in television news and video production in the public and private sectors. She spent five years as a television news reporter, photographer and video editor for the NBC affiliate in Sioux City, Iowa, and the CBS affiliate in Madison, Wisconsin, where she ran the station's news bureau. As a general assignment reporter, Lauri covered a broad range of news events ranging from human interest stories to crime and business news.

During her six years as a producer and writer for Iowa Public Television, Lauri created award-winning educational content for K—12 schools and produced content for the local programs, Student Voices and Zoom Iowa. She also produced and hosted live, interactive field trips using video conferencing technology. A familiar face to Iowans, Lauri is a past host for Festival, IPTV's fundraising broadcast.

Lauri earned her bachelor's degree in journalism and mass communications from Iowa State University.

**Marcia Austin**

Senior Vice President, Hill + Knowlton Strategies

[Marcia.austin@hkstrategies.com](mailto:Marcia.austin@hkstrategies.com) | Direct (813) 755-6201 Mobile (813) 690-3208

---

Marcia Austin is head of the national provider asset group within Hill+Knowlton Strategies' U.S. healthcare practice. The group serves a wide variety of healthcare providers across the primary care, acute and post-acute care continuum. She is also a member of H+K's national crisis and media training groups. In her 20+ years at H+K Strategies, Austin has worked on a variety of high-profile healthcare crisis projects including medical error, data breaches, qui tam, and criminal investigations. Her experience in the interplay between the legal strategy and public accountability is a critical factor in her crisis work.

Austin has an MBA in health administration and is a member of the Society for Healthcare Strategy and Market Development of the AHA. She and her team have been recognized for the quality of their healthcare work by local, regional and national organizations. Austin started her career as a print journalist and hosted a weekly television show in her spokesperson role for a professional sports team.

# TECHNOLOGY & DATA PROTECTION FORUM

## The Regulatory and Enforcement Landscape: Insight from the Insiders

*Deborah Gilg*

*U.S. Attorney, District of Nebraska*

*Dan Birdsall*

*Assistant Attorney General, State of Nebraska*

*James Craig*

*Special Agent, FBI*

*Greg Hollingsead*

*Protective Security Advisor, Department of Homeland Security*

*Moderated by*

*James E. O'Connor and Vickie B. Ahlers*

## Notes

---

**Deborah Gilg,**  
U.S. Attorney, District of Nebraska

---

Deborah R. Gilg, was appointed by President Barack Obama on October 1, 2009 as the 32nd United States Attorney for the District of Nebraska , and the first female United States Attorney for Nebraska. Prior to her appointment, Ms. Gilg served as an elected county attorney in Western Nebraska for sixteen years. In recognition of her expertise as a prosecutor, Ms. Gilg was appointed as a deputy county attorney or Special Prosecutor in over twenty-one counties in Nebraska, in addition to maintaining a private law practice.

Ms. Gilg currently serves on United States Attorney General Eric Holder's subcommittee on Native American Issues, Civil Rights Issues, and Terrorism and National Security Issues. In January, 2011, she was appointed by Attorney General Holder to chair a federal task force on Violence Against Native American Women. Ms. Gilg also serves as the chair of the Child Exploitation and Obscenity Working Group and is the U.S. Attorney representative on the Fiscal Planning Committee for Midwest HIDTA.

**Dan Birdsall**

Assistant Attorney General, Consumer Protection Division

Nebraska Attorney General's Office

[Dan.birdsall@nebraska.gov](mailto:Dan.birdsall@nebraska.gov) | (402) 471-3840

---

Dan Birdsall joined the Consumer Protection Division of the Nebraska Attorney General's Office this year. In addition to handling general consumer protection cases, Dan specializes in privacy and data security matters. He received his Juris Doctor, with distinction, from the University of Nebraska College of Law in 2015. While in law school, Dan worked as a law clerk in the Consumer Protection Division, assisting in cases on a wide variety of subject areas, including charities, antitrust, and privacy. He also served as a senior member of the Moot Court Board and in the presidency of the J. Reuben Clark Law Society. Prior to law school, Dan received his Bachelor of Arts in Political Science from Brigham Young University in 2011.

**James Craig**

Special Agent, Omaha FBI, Cyber Task Force

---

Special Agent Craig has been with the FBI since 2005, first serving in an Information Technology support role and was appointed Special Agent in 2008. SA Craig is assigned to the Omaha Division, Cyber Task Force, which is comprised of investigative and computer forensic personnel from the FBI and ten other state and local law enforcement entities from Nebraska and Iowa. The Cyber Task Force investigates unauthorized computer and network intrusions in both the criminal and National Security arenas. Special Agent Craig is the recipient of two prestigious awards, the FBI Directors Award for Most Outstanding Cyber Investigation as the case agent for Operation Trident Breach and The Department of Justice Attorney Generals Award for Distinguished Service.





# B I O G R A P H Y

---

## Gregory Hollingsead

Greg Hollingsead is assigned to the U.S Department of Homeland Security, National Protections and Program Directorate, Office of Infrastructure Protection, Protective Security Coordination Division, as a Protective Security Advisor for the Nebraska District. In this capacity, he is responsible for working with State and local governments and the private sector in the protection of our Nation's critical infrastructure within the State of Nebraska.

Greg was born and raised in Fort Lauderdale, Florida. Greg entered the United States Air Force in 1978 and retired from active duty at the rank of Chief Master Sergeant in June 2004, after 26 years of honorable service to his country. In June 2004, he accepted a position with Headquarters, United States Strategic Command, Office of Command Security, as the Ballistic Missile Defense Security Program Manager.

His education accomplishments include a Bachelor's of Science Degree in Criminal Justice from Troy State University. He is currently completing a Master's Degree in Cyber Security from Bellevue University. In June 1997, Greg graduated from the prestigious Federal Bureau of Investigations National Academy, 185th Session. In September 2007, he completed the internationally recognized American Society for Industrial Security Certified Protection Professional and Physical Security Professional certifications programs.

He is married to the former Linda Caldwell of Omaha, Nebraska for 35 years and they have three children and two beautiful grand-daughters.