Strafford

Presenting a live 90-minute webinar with interactive Q&A

Mobile Device Privacy and Security Compliance for Corporations

Designing and Implementing Policies for Accessing, Monitoring and Protecting Business Data on Portable Devices

TUESDAY, MAY 13, 2014

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Chuck Cosson, Senior Corporate Counsel, Privacy, **T-Mobile**, Bellevue, Wash.

Daniel B. Garrie, Executive Managing Partner, **Law & Forensics**, Seattle and Special Counsel to **Zeichner, Ellman and Krause,** New York

Darren Kress, Director, Mobile Product and Operational Security, **T-Mobile**, Bellevue, Wash.

Elizabeth Rogers, Chief Privacy Officer, **Texas Comptroller of Public Accounts**, Austin, Tex.

Aaron K. Tantleff, Partner, **Foley & Lardner**, Chicago

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-888-601-3873** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

- In the chat box, type (1) your **company name** and (2) the **number of attendees at your location**
- Click the word balloon button to send

Mobile Device Privacy & Security Compliance

May 13, 2014

Aaron Tantleff
Technology Transactions & Outsourcing
Privacy, Security & Information Management
Partner, Foley & Lardner LLP
atantleff@foley.com
312.832.4367

FOLEY & LARDNER LLP

What is BYOD?

- The mobile "**bring your own device**" (BYOD) era is just beginning and organizations need to react and adapt quickly. Driven by new devices in the marketplace (smartphones, tablets, etc.) and increased wireless accessibility, professionals prefer to use devices they are comfortable with to carry out their work.
- The pressure to implement BYOD comes from two main sources:
  1. **Senior executives**
  2. **Generation Y**
- Executives want to enable choice among a mobile workforce. The potential for enhanced
- productivity and economics are compelling reasons to implement BYOD policy.

BYOD: The Basics

- Generally, “mobile devices” refers to mobile phones, smart phones, tablets and specialized mobile computing devices that primarily connect to a wireless carrier for communications. Excluded are traditional portable computing platforms such as laptops and touch screen computers running a laptop operating system (i.e. Windows).
- Mobile devices will normally include a tailored purpose operating system such as iOS, Android, Blackberry OS, Windows Phone, Symbian or a proprietary device OS
- Mobile devices generally include the option to connect to available wireless broadband services in addition to the carrier network
- Many types of mobile devices will be able to download applications from the Internet or proprietary services unless specifically blocked by the device configuration
- Generally, users will be able to synchronize their devices with enterprise applications via desktop/laptop computers and/or wirelessly

Uncharted Territory - Ownership

- Who owns the device?
  - BYOD versus CYOD
- Who owns the data?
  - Does it matter, personal versus corporate data?
- Courts have not addressed unique aspects of BYOD
- No laws specific to BYOD

Business Imperative

- Enabling mobile workers
- 24/7 work environment
- Competitive advantage
- Workplace “perk”
  - Workers more comfortable and productive
- **COST SAVINGS**

Seven Key Risks

Mixing Business & Personal Data

- Data segregation – the future
- Privacy concerns
  - Employee
  - Third parties
- Other “data” – the great American novel
- Location tracking
- Remote wipe

Information Security

- Extending the corporate security policy to BYOD
- Enforcing security policies on BYOD
- BYOD security software
- Remote wipe
- Tracking
- Malware on mobile devices

Software Licensing

- Company software
  - Which applications?
  - What do the licenses say?
- Employee personal software
  - Ex. Microsoft Office Home
- Get ready for audits

Discovery / Border Searches / Seizures

- BYOD are fair game in litigation
  - Employees must understand
- Litigation hold
- Cost of responding to discovery
- Beware at the border
  - Data and devices can be copied or seized

Worker Injuries

- Repetitive stress and other work related injuries can arise from BYODs.
- Disclaim liability
- Urge employees to follow vendor recommendations
- Check insurance coverages

Shared Use of Device

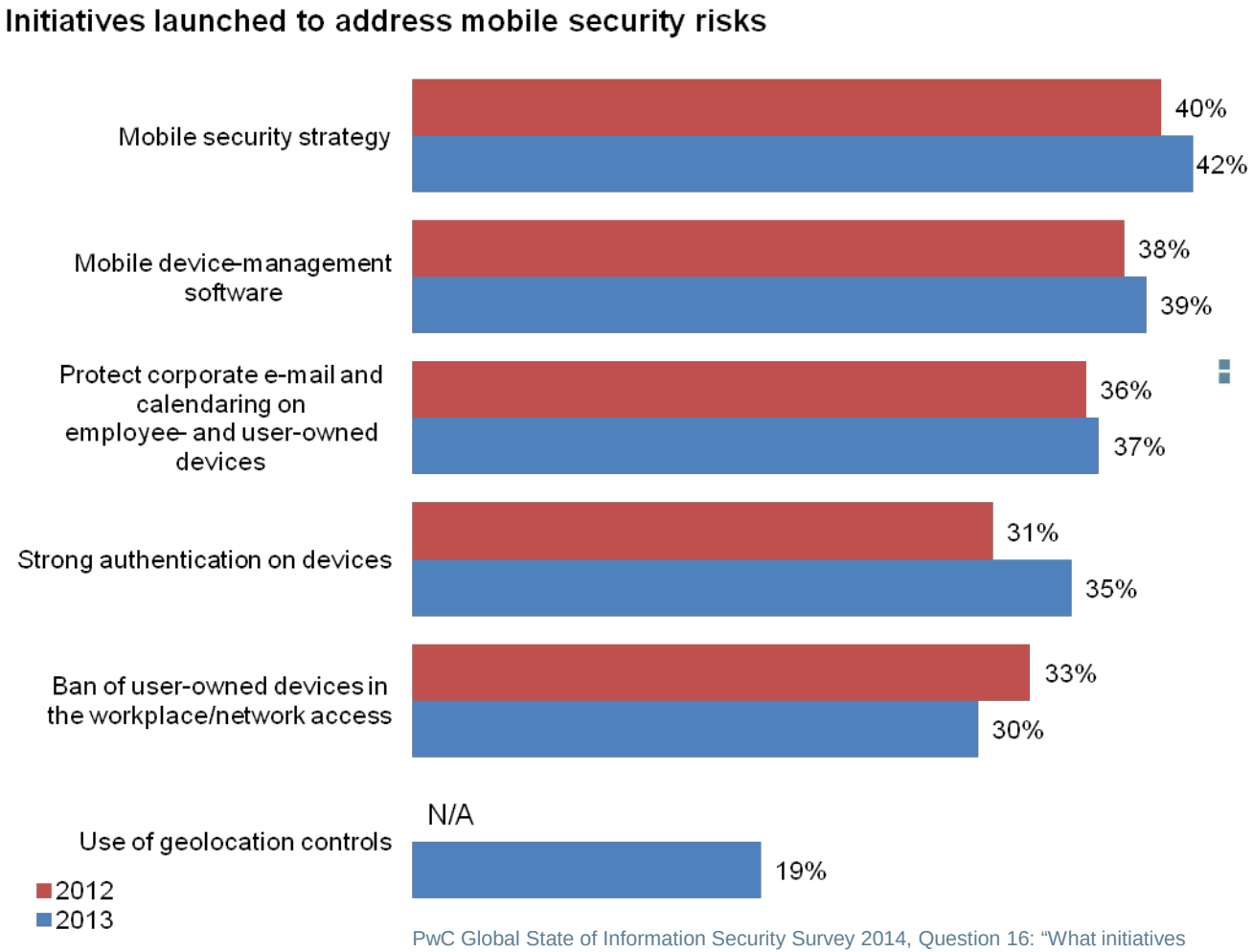
- Friends, family, neighbors, etc.
- A risk that cannot be completely controlled
  - Impossible to obtain consent
  - Policy coverage
- Security implications
- Company proprietary and confidential information at risk
- Privacy and other issues

Employee Disposal

- EOL of BYOD
- The eBay threat, garage sales, Craig's list
  - Army hardware being sold on streets of Afghanistan
  - Broker-dealer Blackberry on eBay
- Company notice of sale or transfer
  - Policy issue
- Terminated employees likely to be reluctant

Challenges

Mobile Security has Not Kept Pace with Deluge of Business Data



PwC Global State of Information Security Survey 2014, Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Smart phones, tablets, and the "bring your own device" trend have **elevated security risks**. Yet efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the proliferating use of mobile devices.

FOLEY & LARDNER LLP

BYOD Trends and Challenges

Employee Trends

- 88% of employed adults use at least one personally owned electronic device for business use[1]

Enterprise IT Challenges

- 1 out of 2 companies have experienced data breach due to insecure devices[2]
- 44% of companies have a mobile security strategy[3]
- 37% of companies employ malware protection for mobile devices[3]

[1]PwC, Consumer privacy: What are consumers willing to share? July 2012

[2]Ponemon and Websense Survey of 4,640 companies, 2012

[3]PwC Global State of Information Security Survey, 2013

FOLEY & LARDNER LLP

Common BYOD Operational Issues

- Use of personally owned devices blurs owner responsibilities regarding **device support**, **ownership of data** and how much **access and control** the organization may have to data on the device
- There is still frequent **resistance by users** to sign acknowledgements or acceptable use agreements (“It’s my device!”)
- **Retention holds** or archive mandates are not considered or applied to BYOD
- Employers may risk **liability** for reviewing certain information stored on an employee’s dual-use device – regardless of policy or consent
- Users have **little incentive to report lost or stolen devices** on a timely basis. In many cases the organization will only learn of a lost device when the user requests access for a new device

Data Collection Challenges

- Some information **resides only on device**, despite potential data flow through the company's server
- Not all devices are created equal, **wide array of devices and software** in the market, requiring different software and tools, depending on the device
- Forensics utilizes both "**physical" and "logical" acquisition of data** - advanced analysis requires obtaining operating system files, device memory and other technical information, plus personal email or documents or phone data
- **Can't just "remove the hard drive**"
- Non-iOS devices may contain an **extra memory card** that needs to be imaged separately from the phone.
- Some devices **do not have in/out ports** (such as USB), difficult to access and remove memory

Data Collection Challenges

- **Data is volatile** – over-the-air device wiping is a risk
- **Lack of employer control** over right to access personal information and data stored on employee-owned devices (home or personal computers, personal email accounts, etc.)
- **Need cooperation and passcode from employee** to access the device - in some cases passwords must be cracked, which can be done, but can be time-consuming
- "Jailbreaking" is typically easier on Android products than Apple, but Android has over 800 types of devices, and Apple is making security improvements to newer OS
- Sometimes devices do not advertise on the device how large (i.e., how much data) they are, so **appropriately scoping the timing of the collection** is not possible
- **Different information** (text, GIS, photos, etc) can be obtained, depending on the device, however it may not be all appropriate for collection, and **may require planning and consent**

Malware Threats Increasing

Source: Juniper Networks, Third Annual Mobile Threats Report 2013

FOLEY & LARDNER LLP

BYOD Security Challenges

- Enthusiasm for newer device types and services, such as the iPad and cloud services, has run far ahead of security. Often these new technologies are not included in overall security plans, even though they are widely used.
- An important aspect is to **set appropriate expectations** with the employee regarding what will happen in a security incident involving a BYOD device.
- The employee needs to immediately report when a device used under the BYOD plan is lost or believed to be otherwise compromised, just as if it were a corporate device, to **allow the device and service to be wiped of any organizational data and to prevent continued access to any organizational resources**.

Lost or Stolen Devices #1 Threat

- 56% of us misplace our ***mobile device*** or laptop each month
- 113 ***mobile phones*** are lost or stolen every minute in the U.S.
- 120,000 ***mobile phones*** are lost annually in Chicago taxi cabs
- 25% of Americans lose or damage their ***mobile phone*** each year
- Major city transit authorities receive over 200 lost items per day

FOLEY & LARDNER LLP

Unique BYOD Investigative Challenges

- Particular risk and difficulty in highly regulated industries
  - HIPPA
  - PCI-DSS
- Need access to data (email, SMS messages, etc) on mobile devices
  - Does IT possess capability to capture data?
  - Explicit right to examine employee devices
- Keep up with ever changing technologies
  - Users want “latest and greatest”
  - Forensic tools unable to keep up with nuances of mobile devices and changes in the market
  - Unable to accurately estimate collection times
  - “Cloud” collections may involve contractual limitations

Contact and Questions

Aaron Tantleff

Technology Transactions & Outsourcing

Privacy, Security & Information Management

Foley & Lardner LLP

321 North Clark Street, Suite 2800

Chicago, IL 60654

Partner

312 832 4367

atantleff@foley.com

FOLEY

FOLEY & LARDNER LLP

Mobile Device Privacy & Security Compliance for Corporations
Strafford Legal Seminars - May 13, 2014

Chuck Cosson
Sr. Corporate Counsel, Privacy
Chuck.Cosson@T-Mobile.com

Darren Kress
Director, Mobile Product and Operational Security
darren.kress@t-mobile.com

Perspective From a Telecoms Corporation

- **(Chuck)** - Legal considerations
  - Respecting Employee Privacy
  - Maintaining Corporate Information Security
  - Tips for Employers: Notice, Policies, Enforcement
  - FTC regulation of data security

- **(Darren)** - Implementing Mobile Security
  - Mobile threats that corporations have to deal with
  - Specialized solutions; responses to threats
  - How carriers improve data security for customers

Legal Considerations

- Legal Context for Corporate Mobile Security:
  - Computer Fraud and Abuse Act
  - Electronic Communications Privacy Act
  - Common Law Privacy Issues
- Elements of Compliant Responses
  - Employee Notice
  - Acceptable Use Policies
  - Issue Checklist

Elements of Compliant Responses

- Notice
  - Communicate internally so as to ensure adequate notice
  - Require BYOD employees to agree to policy
- Policy Elements
  - Detail expectations of privacy when on company systems
  - Expressly provide for investigative access to data
  - Detail security requirements:
    - Allow “jailbroken” or “rooted” devices?
    - Require security software or PIN locks?
  - Explain what happens when:
    - Device is lost or stolen
    - Employee leaves the company
    - Any protective software is not installed or uninstalled

FTC Regulation

- **FTC has authority over "unfair" and "deceptive" practices; enforced in context of data security**
  - **"Unfair" = primarily, a practice causing consumer harm;**
  - **"Deceptive" = practice does not live up to promise**
- **FTC expanding fact-finding on mobile security**
  - **Four areas of ongoing interest:**
    - **Secure Platform Design**
    - **Secure Distribution Channels**
    - **Secure Development Practices**
    - **Security Lifecycle and Updates**
  - **For more see 2013 FTC Mobile Security Forum transcript[1]**

1http://www.ftc.gov/sites/default/files/documents/public_events/mobile-security-potential-threats-solutions/30604mob_0.pdf?utm_source=govdelivery

Mobile Threats to the Corporation

Network
- Unauthorized network access
- Cloud data storage and authentication
- Unencrypted communications

Device
- Rooting
- Jailbreaking
- Lost or stolen device
- Physical manipulation
- SIM card attacks
- Baseband attacks
- DoS attack against the device

User
- Insider data leakage
- Unskilled user / social engineering
- Excessive charges / Fraudulent transactions
- Mobile malware / Spying software / Mobile botnet

Applications
- Poor Authentication and Authorization
- Insecure local data storage
- Client side injection
- Improper session handling
- Security decisions via untrusted input
- Side channel data leakage
- Broken cryptography
- Hard-coded sensitive information
- Malicious code execution
- Privilege escalation
- Insecure user interface
- Bypassing DRM
- Wallet misuse / mCommerce

Services
- Misuse of remote administration
- Unsatisfactorily implemented wipe method

Threat Mitigations

- Policies and Standards
- End-user awareness
- Default security settings
- Apple Activation Lock / Android Device Manager
- Mobile Device Management
- Mobile Application Management
- Restrict access based upon need-to-know
- Security Development Life Cycle
- Compliance monitoring and audit

Carrier Derived Mobile Protections

- Device and application updates
- Default device security settings
- Endpoint protection software
- Encrypted communications
- Commitment to “Kill-switch”
- SIM, Secure Boot, and Trusted Execution Environment (TEE)
- Malicious activity detection and response
  - Fraud
  - Denial of Service
  - Intrusion attempts

MOBILE DEVICE PRIVACY & SECURITY COMPLIANCE

"Public Sector Concerns"

Webinar for Strafford Publications

May 13, 2014

By

Elizabeth C. Rogers

Chief Privacy Officer

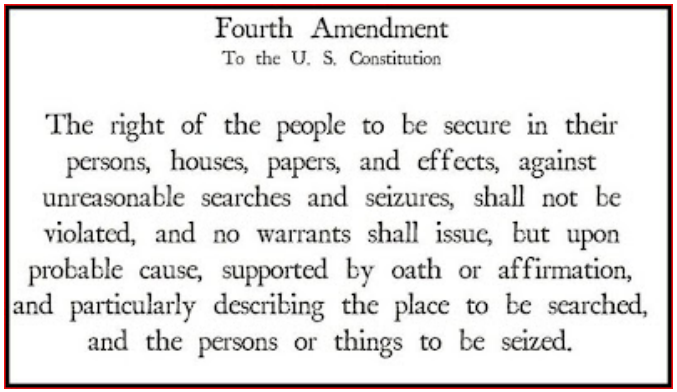
Texas Comptroller of Public Accounts

Traditional Considerations

What are the reasonable expectations of privacy?

- Who owns the mobile device?
- Who is searching or monitoring the device?

What is a reasonable search in the Public Sector?



Fourth Amendment
To the U. S. Constitution

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

- Public sector employees have Fourth Amendment protection against unreasonable searches and seizures because their employer is considered to be a "government actor."
- In the public sector, the Fourth Amendment's protection extends beyond criminal searches.
- "The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by offices of the Government," without regard to whether the government actor is investigating crime or performing another function. Skinner v. Railway Labor Executives Assn., 489 U.S. 602, 613-14 (1989)

Reasonable Expectations of Privacy on Public Sector Issued Devices

- The Supreme Court settled the question of "reasonable expectations" for government issued devices in ***City of Ontario v. Quon***, 130 S. Ct. 2619 (2010). In this case, the Police Department for City of Ontario, CA gave pagers to members of its SWAT team. Before issuing them, the City announced that employees would not enjoy an expectation of privacy regarding the data sent and received via those pagers. Quon sent text messages via this pager and exceeded the monthly allotment of texts.

- The OPD contacted the pager provider to find out if Quon was exceeding his monthly limit for business reasons or because of excessive personal use. After discovering that many of the texts were personal in nature, as well as sexually explicit, the OPD referred the case to its internal affairs bureau. Quon challenged the search of his texts as unreasonable under the Fourth Amendment.

- Even though Quon was a public employee and had greater protection under the Fourth Amendment, the Court ultimately determined that he couldn't have reasonably believed that his personal text messages, sent from a department-issued PCD, would be protected from audit. Quon, 130 S. Ct. at 2632.

Reasonable Expectations of Privacy on Public Sector Issued Devices

- Last summer, an Ohio District Court refused to dismiss an invasion of privacy lawsuit filed by a former employee against her former employer arising from the employer's search of her personal email account that she hadn't deleted from her employer provided device before she separated from employment.

- In ***Lazette v. Kulmatycki***, N.D.Ohio No. 3:12CV2416, (June 5, 2013) Verizon Wireless provided a blackberry for Lazette's use. VW allowed Lazette to also use the company phone for personal email. In September 2010, Lazette left Verizon and returned the phone to her supervisor without deleting her personal Gmail account from the phone.

- Eighteen months later, Lazette learned that Kulmatycki had been accessing her Gmail account and disclosing the contents of the emails he had accessed. Lazette had neither consented to nor authorized Kulmatycki's secret reading of her personal emails.

- Lazette changed her password after she learned about his actions. Before she did so, however, Kulmatycki had accessed 48,000 e-mails in her Gmail account. The emails included communications about her family, career, financials, health, and other personal matters.

- PCD, would be protected from audit. Quon, 130 S. Ct. at 2632.

- Lazette brought suit against Verizon and Kulmatycki, alleging violations of the Stored Communications Act. This statute prohibits intentionally accessing without authorization a "facility" (such as an email server) through which electronic communications are provided. Verizon moved to dismiss the complaint on the grounds that Kulmatycki had authority to access Lazette's Gmail account because the phone was a company-owned blackberry and Lazette had implicitly authorized his access.

- The court rejected Verizon's arguments and denied its motion to dismiss. The court held that the mere fact Kulmatycki used a company-owned blackberry to access Lazette's emails did not mean that he acted with authorization to do so. Further, Lazette did not implicitly consent to Kulmatycki accessing her email when she returned her blackberry without having ensured that she deleted her Gmail account. Lazette's negligence in failing to delete her Gmail account did not amount to approval, much less authorization, for Kulmatycki to read her personal emails. The court analogized: "There is a difference between someone who fails to leave the door locked when going out and one who leaves it open knowing someone [will] be stopping by."

Take Aways from Quon and Lazette

- Consistently enforce any conditions for use of any device, whether employer or employee owned (e.g., text limits).
- Don't read emails from employees' personal email accounts without their consent. The simple fact that an employee is using a company-owned phone or computer to access his or her personal emails does not authorize the employer to read those emails.
- Develop a personnel policy that prohibits employees from reading personal electronic communications of their coworkers without consent. Make sure employees understand and follow this policy. Conditions of consent should be reasonable and specific.
- Have employees return their company-owned phones directly to the IT department rather than the employees' supervisor, and ensure that any personal information regarding the employee is removed before the device is reissued.
- Provide conspicuous notice if there should be no expectations of privacy in any communications contained on a company owned device.

Traditional Privacy Notions Involving Personal Devices: Public and Private Sector Employees

- **General Rule**: Employers cannot monitor or obtain texts and voicemails on an employee's personal cell phone. A different analysis applies, however, if an employee is spending a lot of time at work loudly talking about personal matters Then, there would be a good argument that it wasn't private and the employee can be disciplined for not working.

- **Sunshine Laws Exception**: Texas legislature passed a law in 2013 that makes any state business communications by a state employee, that are conducted on a personally owned device, to be subject to the Public Information Act.

Carrying Company and Personal Information on the Same Device: BYOD and Containerized Solutions on Employer Provided Device

Communicate expectations of privacy clearly and conspicuously:

- Generally employees will assume that they enjoy a reasonable expectation of privacy in the personal content that is stored on the device. Therefore, clear expectations of privacy must be published. If there are none, then make sure that the employees are aware at the inception of device use and again, upon separation of employment.
- Employees should be given conspicuous notice and opportunity to consent to Remote Wipes and Duty to Cooperate with Phones incident to a litigation hold, work-related investigation or request to produce records under the Public information Act.

Containerized Solutions on a Company Owned Device:

- Employers should provide clear expectations of privacy to employees who have the right to keep personal content outside of the work container.
- Even though the device is company provided, the employee may have a greater expectation in the area of the phone that permits personal content.

For example, private email accounts that are password protected generally should not be monitored because there is a reasonable expectation of privacy

- However, employers should provide notice about the consequences of storing personal content on the same device, under a policy that allows co-mingling of data, like:
    - The employees personal information (including passwords) can be stored during backups
    - The personal information can be viewed by monitoring tools, like DLP, and may not be private at all
- Exceptions would apply however
    - If the employee is conducting any illegal activity on the personal account that must be surrendered to law enforcement or the employer's criminal investigations unit
    - If the employee is conducting a personal outside business on company time
    - Any other violation of company policy is being conducted on the device

Examples of permissible violations of expectations of privacy

Communications sent from work: Several cases involving private emails on employer time and equipment have gone against the employee and determined that the employer's interception or use of an employee's personal emails was permitted because of policies that allowed it and implied consent and/or because the employee was using employer-owned computers or sending the emails from work.

Attorney Communications: Even cases of employees contacting their attorney have gone both ways.

- *Attorney-Client Privilege Preserved*: In ***Stengart v. Loving Care Agency, Inc.*** (New Jersey 2010) an employee emailed her lawyer on a company laptop, but through her personal password protected Yahoo account. The court held the emails were protected by the attorney client privilege, but did not really address the privacy issue (i.e., an email from a personal account on a company laptop).

- *Attorney-Client Privilege Waived:* In ***Holmes v. Petrovich Development Company LLC*** (California 2011) an employee contacted her attorney on a company computer with a company email account. The court found the emails were not protected by either a right of privacy or the attorney client privilege. Using the company account and system waived the privilege, and company policies precluded any expectation of privacy. The employer had issued policies that company machines could only be used for business and gave notice that employees had no rights of privacy in their use of company equipment.

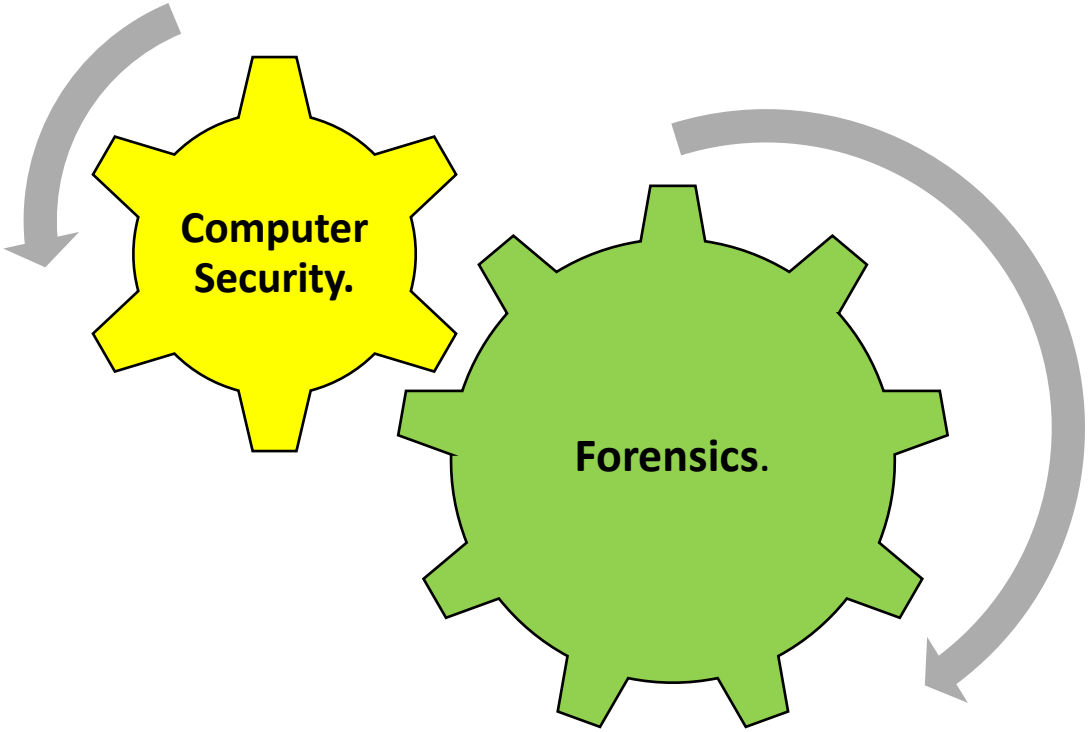
Violation of Employer Policy Against Outside Employment: In ***Sitton v. Print Direction, Inc.*** (Georgia, September 2011), an employer did not violate an employee's privacy rights by accessing an employee's personal laptop to print out personal email messages. The employee had been using his personal laptop at work to help his wife run their printing business. The boss came into the employee's office and saw the computer screen that had a non-work email open. Both the trial court and the court of appeal found that the employer had a legitimate interest in investigating whether or not the employee was running another business from the employer's worksite on the employer's time and found that printing out the emails was proper. The employee had to pay the employer damages for breach of the duty of loyalty.gone both ways.

Overall Take Aways

- Just because you can legally monitor something by law, policy or consent doesn't mean that you should or that it is good management practice.
- If you want a relaxed work environment where employees are trusted and treated as grown-ups, monitoring and discipline over personal phone and computer use will not promote your cause.
- But if you are dealing with sensitive information that requires higher levels of security, then you may need to monitor to protect the business.
- But you can't have it both ways – **Just make sure to clearly and conspicuously communicate the level of privacy that can be expected**.

PRACTICAL TECH ADVICE FOR THE NON-TECHY ATTORNEY.

Everything You Don't Know About E-Discovery (But Wish You Did)



Presented by:

Daniel B. Garrie

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel B. Garrie, Esq.
Executive Managing Partner
Headquarter: Seattle, WA
Offices: Brazil, California, Delaware, Florida, Georgia, New York, Washington

Contact:
W: (855) 529 - 2466
M: (215) 280 – 7033
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

Mr. Daniel Garrie is the Executive Managing Partner at Law and Forensics LLC, a consulting firm that works with clients across industries to address cyber security, cyber warfare, e-discovery, and digital forensics challenges. He is also a General Counsel to Pulse Advisory, a Venture Development firm.

Mr. Garrie has built and sold several Internet security, e-commerce, and search technology startups. Prior to his time at Pulse Advisory, Daniel Garrie was the Worldwide Director of Electronic Discovery & Information Governance at Charles River Associates. He also works as a Strategic Partner for Quorumm Ventures and a Board of Governors member for the Organization of Legal Professionals. He is a nationally recognized educator and lecturer on various topics including computer software, cyber security, e-discovery, forensics, emerging internet and mobile technologies, and cyber warfare. He is the Editor in Chief of the Journal of Law & Cyber Warfare, a fellow at the Ponemon Information Privacy Institute, a distinguished neutral with CPR, and on the editorial board of the Beijing Law Review.

Mr. Garrie recently spoke on the Hill to a Congressional Caucus on the topic of cyber warfare in Washington DC and frequently works with companies all over the world on complex cyber warfare and security related issues.

Digital Forensics

- When digital forensics come into play?
- What is the process of a forensic investigation?
- What should a digital forensic report tell you?

daniel@lawandforensics.com

What is digital forensics?

Digital Forensics is the preservation and analysis of electronic data.

WHY DO WE HAVE TO DEAL WITH DIGITAL FORENSIC ANALYSIS?

In cases where information is hidden, erased, or otherwise altered, digital forensic analysis is necessary to draw further conclusions about the available evidence.

daniel@lawandforensics.com

Applications of Computer Forensics

Employee internet abuse

Unauthorized disclosure of corporate information l

Industrial espionage

Damage assessment

Criminal fraud and deception cases

- FCPA

daniel@lawandforensics.com

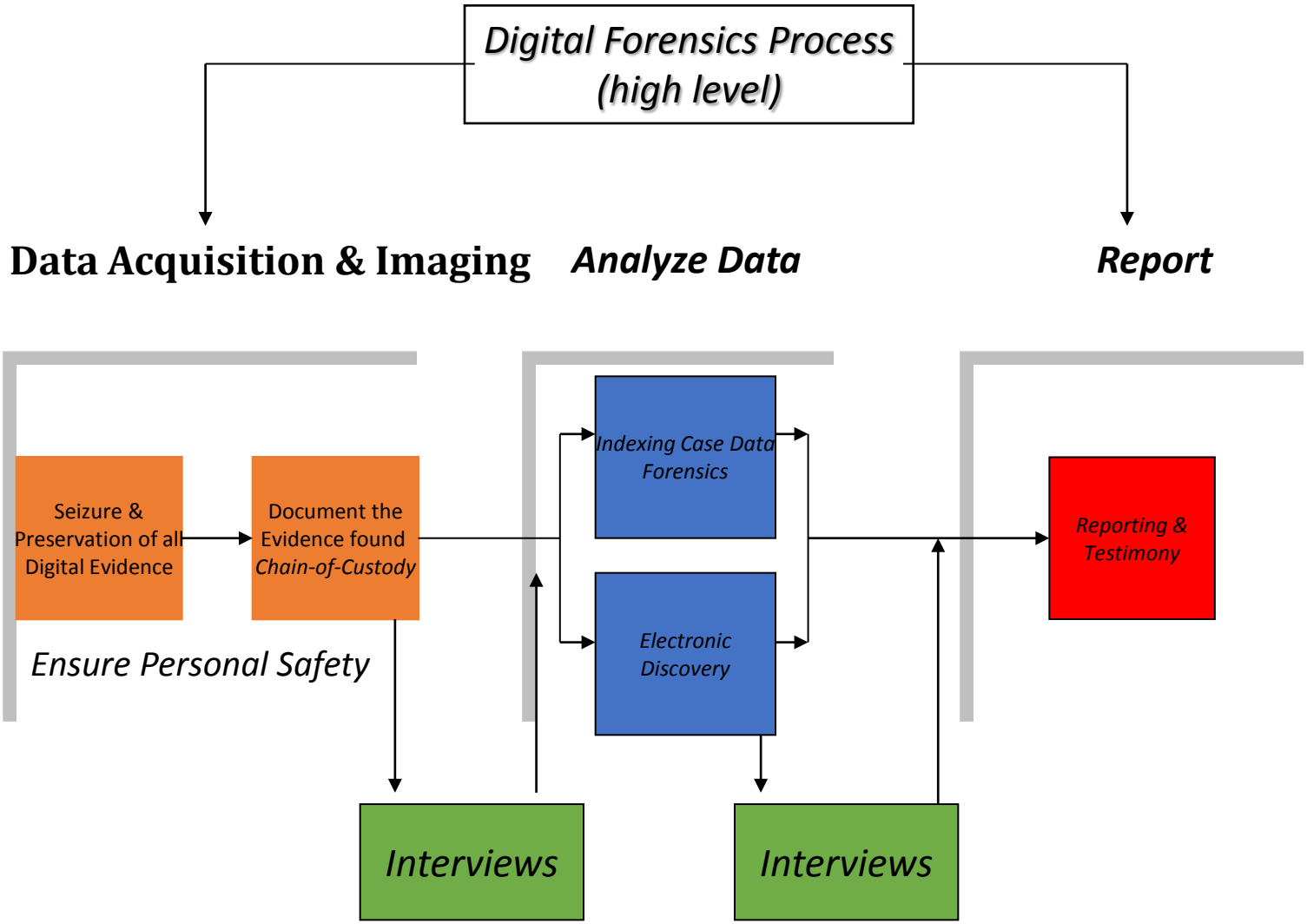
What goes into a forensic investigation?

Digital Forensics in Traditional Forensic Context

Primary substantive data	**The gun and the drugs**	The Hack
Secondary data.	**Fingerprints.**	Hard-drive containing primary data, data trails, and time stamps.
Investigator	**Robbery/Homicide**	Forensic/Malware Examiner

daniel@lawandforensics.com

Details of a Forensic Investigation



daniel@lawandforensics.com

What should be in a forensic report?

Structure of a Digital Forensic Report

1. Brief summary of information
2. Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool
3. Evidence Item #1 (For example A's work computer)
   a. Summary of evidence found on Employee A's work computer
   b. Analysis of relevant portions of Employee A's work computer
      I. Email history
      II. Internet search history
      III. USB registry analysis
   c. Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)
4. Recommendations and next steps for counsel to continue or cease investigation based on the findings in the report

daniel@lawandforensics.com

Devil is in the details

Sufficient Details to Replicate Findings.

Document.	Should document with sufficient detail the steps undertaken by the examiner so that an independent third–party could replicate the conclusions.
Forensic Images.	Forensic images should be available for copying by a third-party. Digital forensic report is less dependable when the forensic images are not available to replicate the findings because of the inability to assess its accuracy or the reliability of its methodology.
Reproducible.	Reports with conclusions that are not reproducible using copies of the forensic images and similar analysis should be granted little credence, and only reviewed in extraordinary circumstances.

daniel@lawandforensics.com

Cyber Security

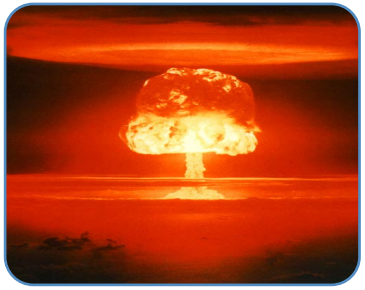
- Technical pieces of cyber security?
- Mobile issues
- Managing mobile devices

daniel@lawandforensics.com

Things to Remember

The time to plan is not at the time of crisis!

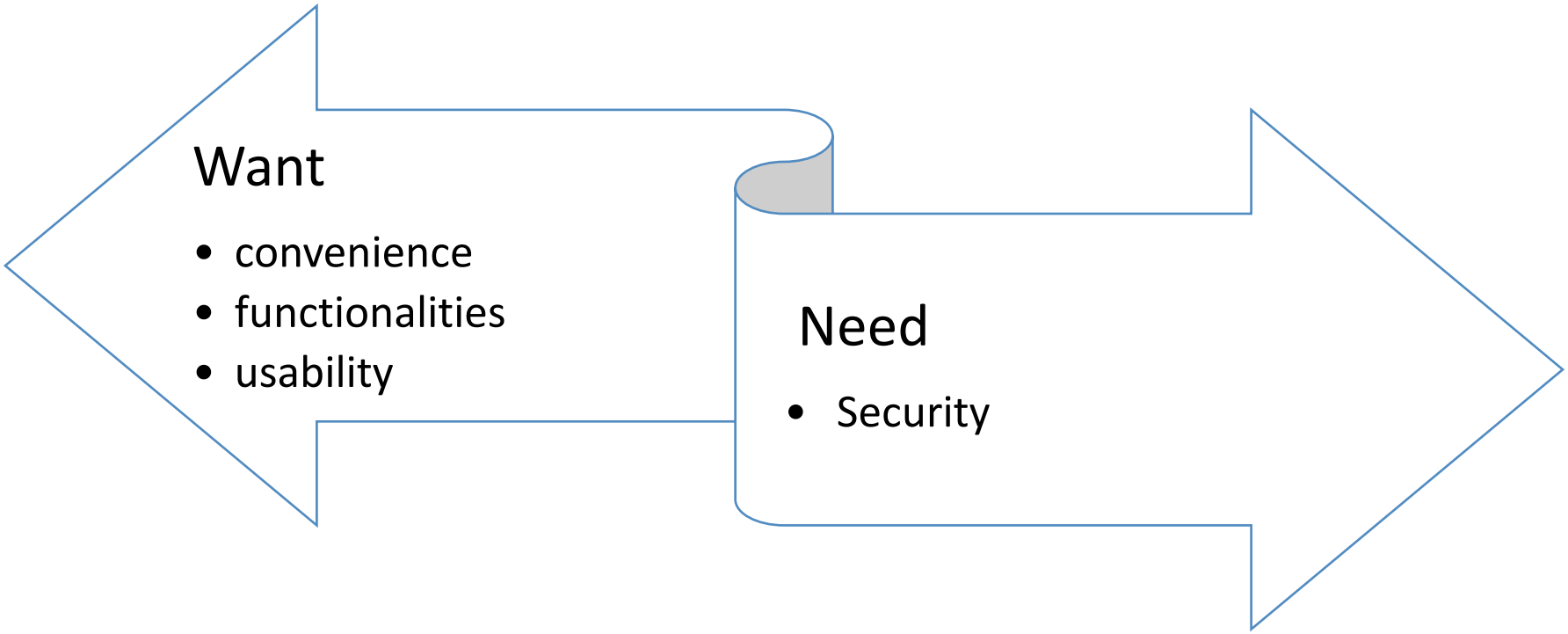
The event causing the problem was most likely not an event that could or was not anticipated!



If it is predictable its preventable!

daniel@lawandforensics.com

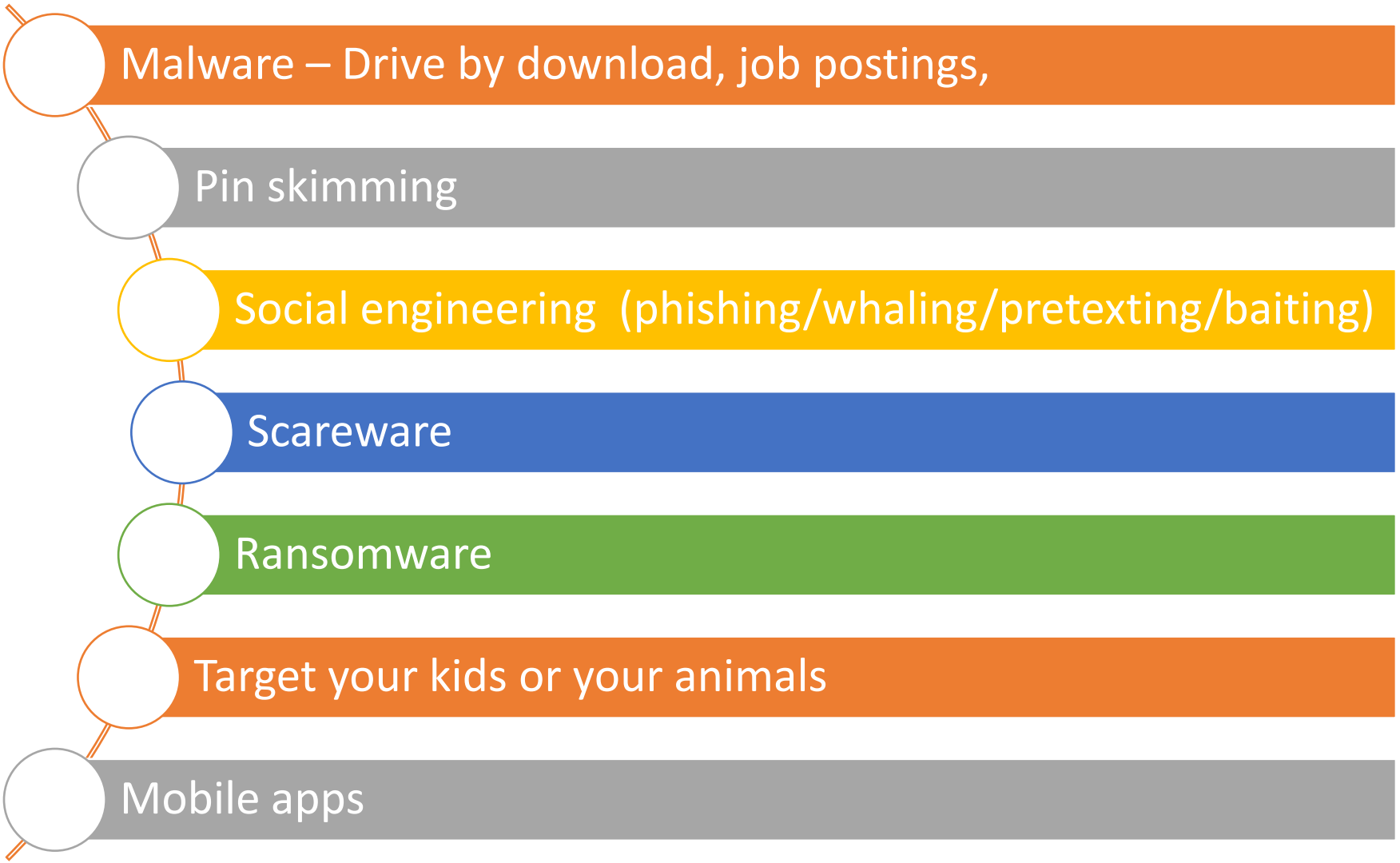
Challenges of Cyber Security



Users want useful and/or fun technology

daniel@lawandforensics.com

How do they get in….



daniel@lawandforensics.com

Checklist for your cyber security readiness

- Firewalls on all public facing networks
- VLAN's and ACL's to isolate the sensitive networks within the enterprise
- Shut down unused switch ports
- Authentication servers to verify and log activity
- Anti-Virus Protection
- Intrusion Detection/Protection systems (IDS/IPS)
- SNMP Monitoring Servers
- Digital certificates

daniel@lawandforensics.com

Law & Forensics LLC
Daniel B. Garrie, Esq.
Executive Managing Partner

Questions & Answers

daniel@lawandforensics.com