MASC Municipal Association of South Carolina℠

Taking Responsibility for Managing Cyber Exposure Risks Within Cities and Other Public Entities

Municipal Technology Association of South Carolina
Spring Meeting – March 23rd, 2017

NetDiligence®

About NetDiligence®

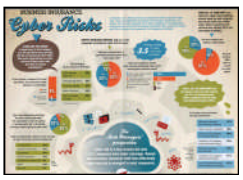
- 15+ years supporting the cyber liability risk mitigation needs of insurers and their clients
- We conduct QuietAudit® cyber risk assessments for organizations – and their vendors – of all sizes & sectors.
- We provide access to our eRiskHub® cyber risk management portal for 80+ carriers, brokers, and risk pool organizations – and tens of thousands of their clients (including the National League of Cities & MASC).
- We build/host Breach Plan Connect® to help clients better organize and access key elements of their incident response plan capabilities.
- We sponsor cyber risk Conferences each year in Philadelphia, Santa Monica, Toronto, and London

Sampling of insurers that we support:

- Aegis
- AIG
- Allianz
- Arch
- Argo
- Aspen
- Axis
- Barbican
- Beazley
- Berkley
- Berkshire Hathaway
- Brit
- Chubb
- Cuna Mutual
- DMI
- Endurance
- Hiscox
- HSB
- Ironshore
- Kiln
- Liberty
- Markel
- National League of Cities
- One Beacon
- Philadelphia
- Principia
- QBE
- RLI
- Starr
- Swiss RE
- Travelers
- Trans Re
- USLI
- Vela
- XL
- Zurich

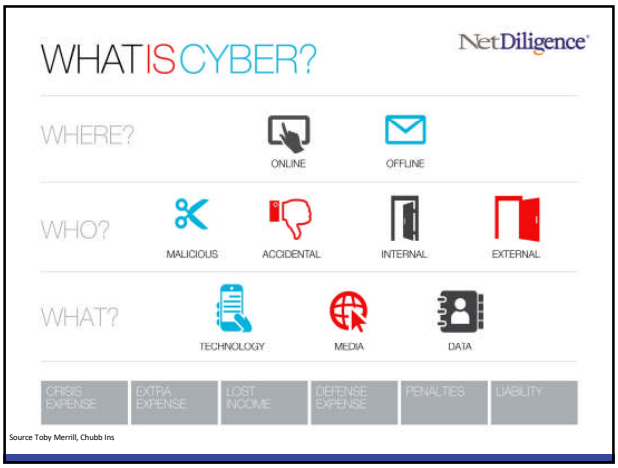
Why Are We Here?

BUSINESS INSURANCE



Risk Mgr Top 5 Concerns	
Cyber security, cyber risk	56%
Changing legislation	53%
Corporate liability	37%
Natural disasters	36%
Talent and skills shortage	33%

NetDiligence®



Cities Engage in Data-Centric Activities

Cities & Other Public Entities are:

- Increasingly dependent on Information Technology for conducting business
- Collecting various types of Constituent sensitive data that may or may not require Confidential protection per current law
- Outsourcing data/applications to Application Service Providers (ASPs) or Public Cloud Vendors to save tax dollars on IT infrastructure requirements
- Replicating data in multiple locations, including via off-site archival storage
- ***Not necessarily implementing effective information security programs to govern these activities***

Cyber Threats Facing Cities (Malicious)

Insiders: Disgruntled Employees

- Changing/deleting data, installation of logic bombs, holding data hostage, compromised backups
- Stealing & selling data

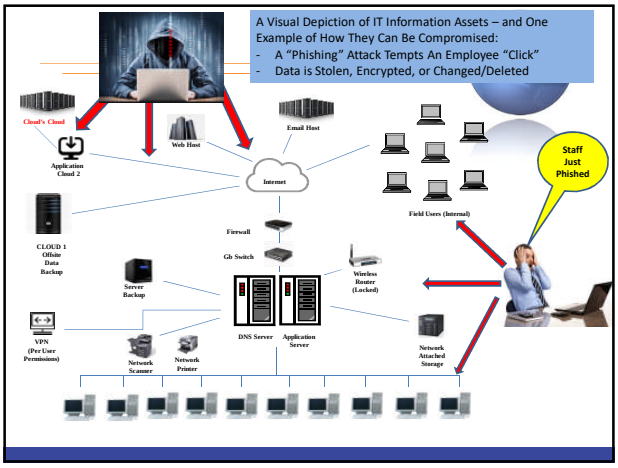
Outsiders: Individuals/Organizations with Malicious Intent

- Active hacking (intrusion, takeover of systems for illicit purposes)
- Distributed denial-of-service (DDoS)
- Political statements or reputational damage
- Social engineering (manipulation of employees via telephone for passwords/data)
- Email hacking (phishing, spear-phishing of executives for data/wire funds)
- Extortion (ransomware – files encrypted and held hostage for Bitcoin payment)
- Other types of virus/malware entries

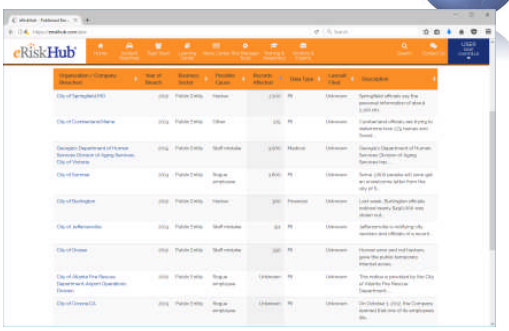
Cyber Threats Facing Cities (Routine)

Employee/Entity Errors, Negligence, Policy Violations, IT Failures

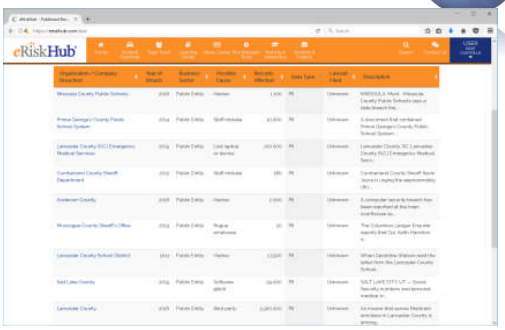
- Incorrect data entry which prejudices Constituents or others
- Lost/stolen laptops, smartphones, tablets, servers, and workstations with data
- Unapproved sharing of data with unauthorized third parties (or other types of employee information security policy violations)
- Improper transmission of sensitive data to authorized parties without encryption or other physical protections
- Failure to adhere to federal, state, or other regulatory mandates regarding privacy data protection (e.g., for Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Cardholder Industry (PCI), or other types of sensitive financial/account information).
- Failure of individual mission-critical systems or applications without adequate fail-over or disaster recovery procedures
- Physical datacenter disasters associated with weather, earthquakes, utility grid failures, or adverse human activities (political, crime, war, disease)



City-Level Experience With Cyber Events



County Experience With Cyber Events



Sovereign Immunity Will Not Spare Costs

South Carolina Department of Revenue Data Breach 2012

- International hacker hit SC DOR for 3.6 million SSNs, 387K credit/debit card numbers, and other sensitive information. A phishing attack directed at SC DOR employees was the entry point for the data thefts that followed
- While the State has avoided class action liability, significant expenses resulted from notification/remediation tasks for the benefit of impacted individuals
- According to a 2014 report by Wells Fargo, the State ultimately paid $1.3 million for notification, $12 million for credit monitoring, and $5.6 million for data encryption improvements (please see: ***https://wfis.wellsfargo.com/insights/whitepapers/Documents/White_paper_Public-Entity-Security.pdf***)
- One positive element: subsequent stepped up oversight and investment in State-level cybersecurity capabilities & governance

Very Common Technical Weak Spots

PROBLEM 1: **Intrusion Detection/Prevention Systems (IDS/IPS) Not Implemented or Poorly Utilized**

- Studies show that 70% of actual breach events are NOT detected by the victim-company, but by 3rd parties – including law enforcement, customers, or other entities – or not at all.
- FTC and plaintiff lawyers will often cite "failure to detect" as a negligence element in their cases.

PROBLEM 2: **Lack of Encryption for Sensitive Data**

- Sensitive data relating to individuals (customers/constituents, employees, business owners) should be encrypted whenever possible in both ***in-transit*** and ***at-rest*** settings – in-transit encryption is very common, but at-rest encryption is much less so
- Oftentimes, entities have not even performed an information asset inventory so as to be able to determine conclusively what sensitive data actually exists – so as to be able to make encryption decisions effectively

Very Common Technical Weak Spots

PROBLEM 3: Patch Management Challenges

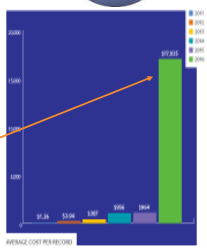
- All systems need constant care – via updates/patches to counteract evolving weaknesses that appear on a continuous basis
- Verizon DBIR 2016: over 85% breaches caused by old/known exploits that were several years old – suggesting that vigilance in this area holds room for improvement

PROBLEM 4: Poor Vendor Management/Accountability for Client Data

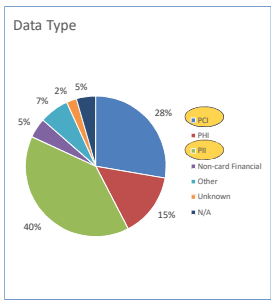
- Vendors are often in the care, custody & control of client systems and data
- Client oversight is often non-existent, or significantly limited to receipt of a statement of security practices followed by the Vendor
- Service Level Agreements (SLAs) often disown security assurances – and prevent Clients from legal/contractual recourse in case of a data breach caused by the Vendor
- Despite these limitations, approximately 1 in 3 reported data breach events involve at least some aspects of Vendor performance/activity

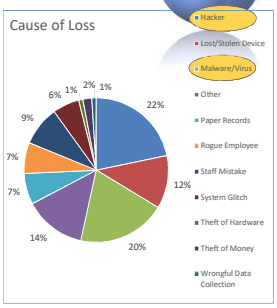
NetDiligence® 2016 Cyber Claims Study

- Sample size = 176 claims
  Detailed partner report now inside your eRiskHub®
- Per Breach Costs
  - **Average breach cost:** $665K
    *Comment: more representative of '**main street**' than Wall St, **Small biz = 87% of claims**.*
  - Large Co: $6M (up from last year)
  - Healthcare: $717K
- Per Record Costs
  - **Average per-record cost**: $17K* *(median = $40)*
    **Spiked average due to 3 big 'outlier' claims; one was over a $1M per record!*
  - **Cost Range**: $0.03-$1.6M *(pennies to million)*



NetDiligence® 2016 Cyber Claims Study





What Can You Do? Pursue *Assessments*

Purpose: Identify Strengths & Weaknesses

- Identify existing practices (or lack thereof) within specific topic areas, including:
  - Information Security Organization
  - Vendor Security Management
  - PCI (credit/debit card transactions)
  - Encryption (in-transit and at-rest)
  - Technical/Compensating Controls
  - Application Security
  - System/Network Operations
  - Business Continuity / Disaster Recovery
  - Incident Response
  - Privacy

What Can You Do? Pursue *Improvements*

Frequent Recommendation Examples:

- Identify a named Information Security Officer, and vest accountability in that person for the effective implementation and enforcement of security-centric policies and practices
- Understand, at a detailed level, where sensitive data exists (and goes) within the course of everyday activity within your city government – and determine how it can best be protected from accidental/malicious disclosure, including via encryption and strong access controls
- If you take credit cards for payment of fees, fines, licenses, records, or taxes, make certain that you and your payment processor are PCI DSS compliant
- Make a greater effort to understand what types of data and functions you entrust to your third-party hosting/cloud providers – and hold them accountable (as much as possible, given market conditions) for effective data protection commitments
- Conduct periodic vulnerability scanning and/or penetration testing of your public-facing environment
- Outsource application development to security-trained vendors

What Can You Do? Pursue *Improvements*

Frequent Recommendation Examples:

- Invest ongoing financial resources in generational upgrades for key security technology solutions – including firewalls, intrusion detection/prevention, anti-virus, etc.
- If your city makes use of smartphones/tablets for remote access by your employees, ensure that you have deployed a contemporary mobile device management (MDM) solution to prevent unauthorized data disclosure via theft/loss of such devices
- Ensure that your disaster recovery plan capabilities and goals match the existing service delivery requirements of your departments and constituents – and that periodic plan testing takes place to ensure those goals can be met
- Implement a documented (and 24x7 accessible) incident response plan program that fosters timely response and remediation efforts
- Train employees on all key elements of security and privacy policy requirements and their adherence to them
- Ensure that your City's Law Director is fully up-to-speed on data privacy laws and your City's obligations in the event of a data breach event.

What Can You Do? Pursue *Cyber Insurance*

Make Sure Your City Carries Cyber Risk Insurance:

- Check with your Risk Manager to ensure that your City has purchased cyber insurance coverage – which exists separate and apart from traditional E&O policy coverage. **Your NLC Risk Pool can play a role here**

Make Use of Additional Loss Mitigation Resources/Services:

- **As a member of MASC**, you are already eligible for **free registration** for up to three members of your City administration to the NLC-RISC eRiskHub. To register for your account, please follow these instructions:
  - **Access https://www.eriskhub.com/NLC**
  - **When prompted for your custom Access Code, please use: 13522**

NetDiligence®

eRiskHub® BreachCoach®

BreachPlan Connect QuietAudit®

Thank you!

Dave Chatfield
NetDiligence®
Dave.Chatfield@NetDiligence.com
954.684.9190