Secure Relocation:
Understanding Data Security

Dave Siegel




- **Siegel Data Management ("SDM") resources bring nearly 100 man-years of global business experience to bear. Resources include former executives from companies in the financial and healthcare verticals, and advisory clients including Blue Cross Blue Shield, Citadel Investment Group, The Northern Trust Company, and Bank Of America / Merrill Lynch.**

- **Dave Siegel**
  - **Former Chief Information Officer for financial services company with $10+ billion AUM**
  - **Former Managing Director of IT/Enterprise Architecture for BCBSA**
  - **Experienced Board Room Advisor; over 30 years engaged in information security, data strategy, enterprise and data architecture, organizational, procedural, and technical improvement**
  - **Led enterprise process and technology analysis and improvement of global leading healthcare insurer**
  - **Architected, designed, developed and optimized data warehouses and information delivery platforms for global leaders in the finance and healthcare insurance industries**




Example Scenario

- HR identifies candidate
- Initiate contact to candidates via email
- Pertinent info is returned via email
- Home sale (PII transferred, banking, SSN, etc.) info sent to RMC
- Clients may email the PII
- Realtors, brokers, inspectors may all be sharing PII info
- Tax provider may be involved
- US/International potentially involved
- Through service partner
- Finally, there will likely be hotel, travel, etc.




Information Security and Cyber Risk

Data Breach:
The "Tip Of The Iceberg"




Information Security and Cyber Risk

- Businesses face all kinds of risks, some of which can cause serious loss of profits or even bankruptcy. But while all large companies have extensive "risk management" departments, smaller businesses tend not to look at the issue in such a systematic way.
- **A data breach is the type of preventable event that can have catastrophic effects on your clients' financial future and your company's stability.**
- **An InfoSec event will often precipitate the following risk types…**




Compliance Risk

- Are you complying with all the necessary laws and regulations that apply to your business?
- You must protect
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
- Laws change all the time, and there's always a risk that you'll face additional regulations in the future. And as your own business expands, you might find yourself needing to comply with new rules that didn't apply to you before.
  - HIPAA, FFIEC, NYS DFS 23 NYCRR 500




Operational Risk

- Traditionally, operational risk refers to an unexpected failure in your company's day-to-day operations. It could be a technical failure, like a server outage, or it could be caused by your people or processes.
- In some cases, operational risk can also stem from events outside your control, such as a natural disaster, or a power cut, or a **data breach**. Anything that interrupts your company's core operations comes under the category of operational risk.
- Operational risks can have a big impact on your company. Not only is there the cost of fixing the problem, but operational issues can also prevent customer orders from being delivered or make it impossible to contact you, resulting in a loss of revenue and damage to your reputation.




Reputational Risk

- There are many different kinds of business, but they all have one thing in common: no matter which industry you're in, **your reputation is everything**.
- If your reputation is damaged, you'll see an immediate loss of revenue, as customers become wary of doing business with you. Your employees may get demoralized and even decide to leave. You may find it hard to hire good replacements, as potential candidates have heard about your bad reputation and don't want to join your firm. Advertisers, sponsors or other partners may decide that they no longer want to be associated with you.
- Reputational risk can take the form of a major lawsuit, negative publicity about you or your staff, or high-profile criticism of your products or services. And these days, it doesn't even take a major event to cause reputational damage; it could be a slow death by a thousand negative tweets and online product reviews.




Data Breach 101

- Who perpetrates the breach?
- What causes the breach?
- When does the breach occur?
- Where does the breach occur




Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target




How do you prevent a breach?

- Education and awareness is vital.
- Internal – train and verify. Hold staff accountable.
- External – engage expertise, run vulnerability scans, simulate a phishing attack and analyze responses, protect your perimeter, know your 3rd and 4th parties' level of preparedness.




This is NOT a "One And Done"

- Information security and cyber preparedness must be an active endeavor; run periodic assessments and audits.
- The perpetrators are similar to a quickly evolving pathogen.
- Complacency is akin to leaving your keys in your car with the doors unlocked – eventually something very bad (and preventable) will happen!
- Secure your data "at rest" and "in flight".
- Use/provide secure VPN (virtual private network) connectivity to your staff and clients.
- Implement and govern data retention AND destruction policies.




Example Scenario – Where Are The Gaps?

- HR identifies candidate
- Initiate contact to candidates via email
- Pertinent info is returned via email
- Home sale (PII transferred, banking, SSN, etc.) info sent to RMC
- Clients may email the PII
- Realtors, brokers, inspectors may all be sharing PII info
- Tax provider involved
- US/International potentially involved
- Through service partner
- Finally, there will likely be hotel, travel, etc.




Questions and Comments?

WiERC
WISCONSIN EMPLOYEE RELOCATION COUNCIL

CRC CORPORATE RELOCATION COUNCIL of chicago

Contact information:

Dave Siegel
Dave.Siegel@SiegelDataMgmt.com
847.644.5158