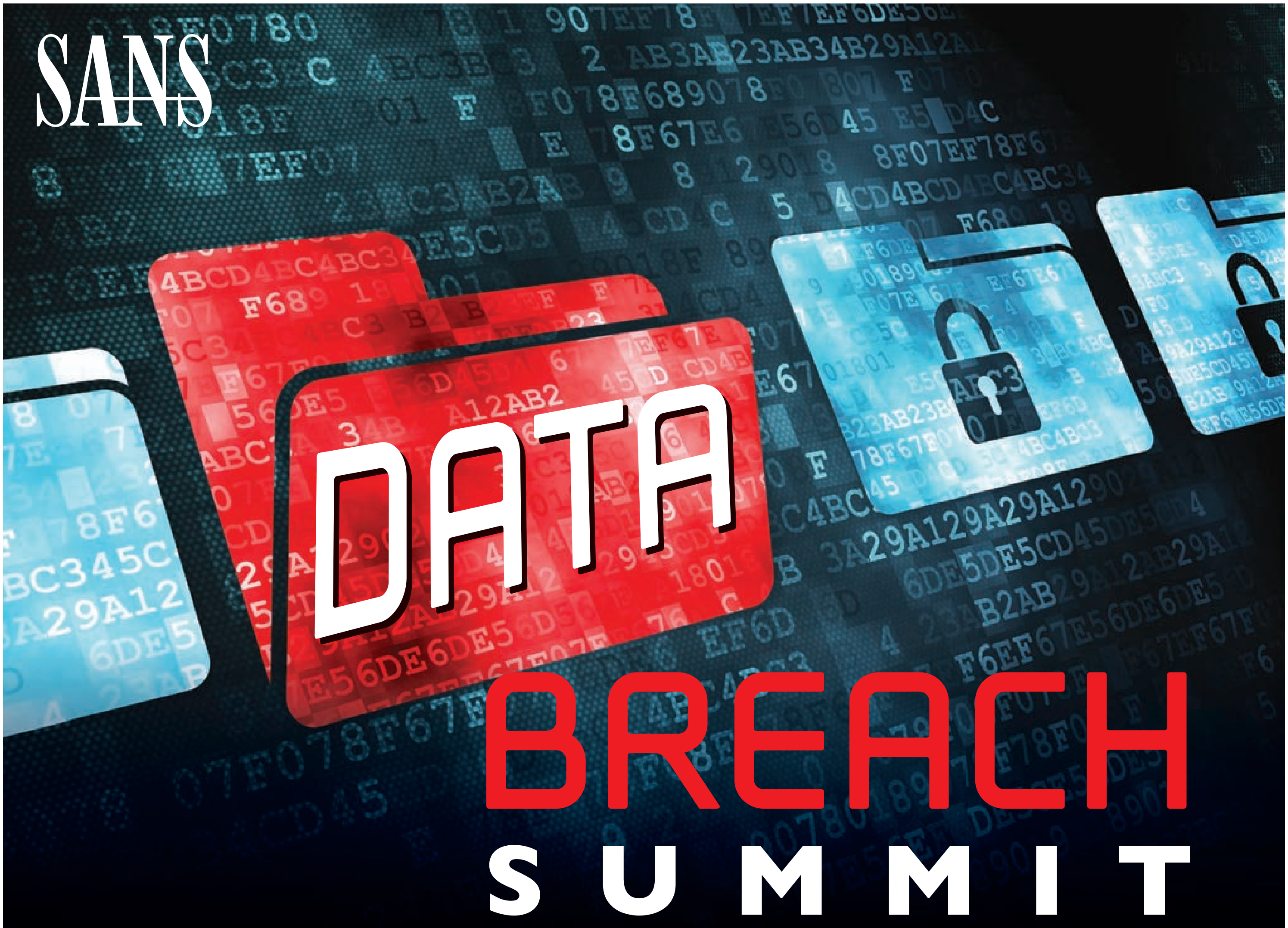
SANS



DATA BREACH SUMMIT

Program Guide

@SANSDefense #SANSDataBreachSummit

Benjamin Wright

Welcome to the **Data Breach Summit**! As we come together as a community to discuss and share ideas on security incidents and breaches, your participation is what makes our Summit uniquely valuable. We have assembled diverse members of the community, including top industry experts sharing their wisdom on the latest trends and most challenging issues. Our goal is for you to take away actionable information, which you can use to prepare for and respond to possible security breaches.

Take this opportunity to introduce yourself to those sitting around you, join one of the many conversations during breaks, and engage with our expert speakers during our networking events.

Finally, let's have fun and make this day count! Attendees tell us time and time again that the greatest value of our Summits is the interaction with others and the newly forged connections made during the time with us.

Looking forward to an amazing day!

Benjamin Wright
Attorney
SANS Institute Instructor, "Law of Data Security and Investigations"

P.S. Nothing communicated during the Summit constitutes legal or other professional advice for any particular situation. If you need legal or other professional advice, your organization should consult its own advisors.

Agenda

All Summit Sessions will be held in the Buckingham Ballroom (unless noted).

All approved presentations will be available online following the Summit at
http://cyber-defense.sans.org/resources/summit-archives
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Thursday, August 18

7:00-8:30am	**Registration & Coffee** (LOCATION: BUCKINGHAM PRE-FUNCTION
8:30-8:50am	***Welcome, Overview & Summit Roadmap*** Every day, the modern enterprises encounters security events that must be investigated. For a few of those events, full investigation finally reveals that the enterprise has suffered a data breach that entails legal and public obligations. Although experts like lawyers and investigators will have opinions, it ultimately falls to management to made decisions on the investigation and the response, including tradeoffs between legal confidentiality and public communication. This Summit aims to improve the wisdom available to management in its decision-making process. ***Benjamin Wright**, Esq., Senior Instructor/Summit Chair, SANS Institute*
8:50-9:25am	***Two Truths and a Lie About Data Breaches*** Are you adequately prepared to handle a data breach crisis? Jeff will discuss the latest trends in enterprise data breaches and present a model for assessing your organizational readiness for a potential breach. Included in the presentation will be current spending patterns to address security (including insurance and breach preparedness) and a checklist of best practices for reacting to and communicating about a breach. ***Jeffrey Louie**, Retired Director of Global Informatics Services, Agilent Technologies*
9:25-10:00am	***Incidents and Breaches: The Executive Management Decision-Making Process*** A large university system possesses many different types of sensitive data, including patient records, student records and financial data. It faces many legal and political expectations for securing data and communicating to the public if security is compromised. Mr. Segran will outline the challenges management faces as it evaluates input from experts about a possible compromise. He will share lessons learned in his experience as both a university CIO and a leader in state government cybersecurity. ***Sam Segran**, CIO, Texas Tech University*
10:00-10:20am	**Networking Break and Vendor Expo** (LOCATION: FRANK LLOYD WRIGHT)

Thursday, August 18

10:20-10:45am

To Call or Not to Call?: Implications and Obligations of Involving the FBI

As an enterprise discovers it has experienced a serious security incident, it must evaluate with legal counsel whether and how to contact law enforcement agencies such as the Federal Bureau of Investigation. Mr. Leatherman will address what it means in practice for the FBI to engage in a cyber security investigation at an enterprise such as a private corporation. Topics may include confidentiality of the investigation, process for cooperation between the enterprise and the Bureau, and what influence the enterprise may have over the direction and scope of the Bureau's investigation.

***Brett Leatherman**, Section Chief – Cyber Outreach Section, Federal Bureau of Investigation (FBI)*

10:45-11:20am

Legal Responsibilities for a Data Breach

With 47 different state statutes, federal laws, and contractual obligations, unraveling the legal requirements of a data breach successfully can be an incredibly complex endeavor. Learn how to navigate the complexities of these laws, when to ask for assistance, and what activities may draw regulatory scrutiny or litigation.

***Melissa Ventrone**, Partner; Chair - Data Privacy & Security Practice Group, Thompson Coburn*

11:20am-12:15pm

How to Determine the Significance of a Security Incident

Security incidents are common. But only a few of them constitute "data breaches" or other significant compromises of security. These panel members will share the wisdom they have gained by evaluating incidents in healthcare and other industries.

MODERATOR: ***Benjamin Wright**, Esq., Senior Instructor/Summit Chair, SANS Institute*

PANELISTS: ***Rick Kam**, President/Co-Founder, ID Experts*
***Meredith Phillips**, Chief Information Privacy & Security Officer, Henry Ford Health System*
***Erika Riethmiller**, Director, Corporate Privacy-Incident Program, Anthem, Inc.*

12:15-1:15pm **Networking Lunch** (LOCATION: BUCKINGHAM BALLROOM)

1:15-1:45pm

Breach Detectives: Gathering and Assessing Evidence of Incidents and Breaches

Digital evidence can be tricky and subject to conflicting interpretations. The evidence of a possible breach can come from many sources, including third parties such as vendors or customers. This panel will examine how to find, preserve and understand the evidence.

MODERATOR: ***Benjamin Wright**, Esq., Senior Instructor/Summit Chair, SANS Institute*

PANELISTS: ***John Mohr**, Chief Information Officer, MacArthur Foundation*
***Jake Olcott**, VP, BitSight*

1:45-2:15pm

Relationship Management: Effectively Partnering with Your Cyber Insurer

Cyber Insurance is a unique and growing coverage. The risk can vary greatly from one insured company to another. This session will address what an insurer needs to know at the outset about risk at the insured company, as well as what actions the insured needs to take if it suffers a breach.

***David Hallstrom**, Practice Leader – Information Risk, CNA*

Thursday, August 18	
2:15-2:40pm	***Real Breach Stories from the Trenches*** We often read or hear about data breaches in various news outlets, but by the time the general public learns of the incident, it is third- or fourth-hand news. In this panel discussion, listen first-hand to real-life incidents in varying verticals handled by front-line experts in forensics, public relations and remediation who assist breached entities every day. ***Rich Blumberg****, Director, Data Breach Response, IDT911* ***Ondrej Krehel****, Digital Forensics Lead, CEO and Founder, LIFARS LLC* ***Jamie Singer****, Sr. Account Supervisor – Corporate Reputation & Risk Management, U.S. Data Security & Privacy Group, Edelman*
2:40-3:00pm	**Networking Break and Vendor Expo** (LOCATION: FRANK LLOYD WRIGHT)
3:00-3:20pm	***Overview of Afternoon Exercise*** Learning comes from doing. The attendees will break into small discussion groups. Each group will be assigned a fact scenario and asked to develop a plan of action. The exercise will emphasize collaboration among experts such as CISOs, lawyers and risk managers. Speakers from earlier in the day will participate. ***Benjamin Wright, Esq****., Senior Instructor/Summit Chair, SANS Institute* ***John Wurzler****, President, OneBeacon Technology Insurance*
3:20-4:30pm	***Ready...Set...Respond: Workshopping the Inevitable*** Attendees will work through a hypothetical but realistic breach scenario in small groups. Each scenario will raise legal, investigative, management and communications issues. *See next page for more information on scenarios.*
4:30-5:00pm	***Group Presentations: Pulling the Lessons All Together*** The plenary conference will reconvene for open discussion. Discussion groups will share lessons with all attendees. The goal is to improve practices in investigations, communications and compliance with law.
5:00-5:15pm	***Summary/Closing Remarks***

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.

@SANSDefense #SANSDataBreachSummit

General Questions

These are general questions that can inspire discussion in each fact scenario.

- *What should be management's game plan as the initial facts come in?*
- *What are the questions management should be asking, and how should management get the answers?*
- *How would you change or expand the scenario to make it more challenging? What would be the implications or new questions raised by the change?*
- *What is the role of insurance?*
- *When should management engage an outside expert or seek a second opinion?*
- *What does management now wish it had done before the scenario transpired?*
- *How should management separate truth from mere speculation or outright misinterpretation of the facts?*
- *When and how should law enforcement be involved?*
- *If your group has extra time, or does not like a scenario assigned to it, make up another scenario.*
- *How might legal requirements differ from what is the right thing to do from a consumer protection and PR perspective?*
- *What are best practices with regards to documentation for incident handling?*
- *What should be the protocols for interactions among the IT department, the legal department and the privacy department? Should IT notify legal and privacy every time it sees an alert?*

Ten Fact Scenarios – Five Groups

BLUE GROUP – FIRST SCENARIO

College of Engineering (CoE) Data Breach

- Greater Renegade University (GRU) is a large university that conducts extensive research activities.
- GRU also has collaborations with a medical school for a bioengineering program (potential for PHI data). However, PHI data is not stored on GRU's network.
- GRU processes credit card transactions using GRU's centralized payment gateway. Credit card data is contained within a separate PCI network managed by central IT.
- Central IT manages the network for all colleges (that is, departments within GRU) except for the College of Engineering (CoE).
- All colleges use GRU's central network ID except for CoE.
- CoE manages its own network, and it runs a separate network ID system for the CoE network.
- Faculty in CoE conduct sensitive research leading to new technology and other federal research, including sensitive Department of Energy research.
- The IT Security Office is housed in the CIO's Office under central IT.
- The Dean of CoE reports to the Provost, who reports to the President.
- The CIO also reports to the President.

Incident:

- The College of Engineering has been the target of sophisticated cyberattack(s).
- GRU President was alerted by the FBI to a cyberattack of unknown origin and scope on the College of Engineering network by an outside entity. As soon as the FBI alert was received, the President's Office notified the Provost and the CIO. The Dean of CoE and the CIO were tasked by the President and Provost to investigate.
- The investigation revealed the presence of a previously undetected, sophisticated threat actor on the CoE network.
  - A prominent security vendor said the attacks came from attackers based in China, who use advanced malware to attack higher education.
  - The investigation also revealed that the earliest known date of intrusion on the CoE's network was 9 months ago.
- The College of Engineering's network was disconnected from the Internet and from the rest of the University. A large operation is underway to securely recover all systems.The outage is expected to last for several days, and the effects of the recovery tasks are largely limited to the College of Engineering.
- The investigation revealed that malware was found on two dozen systems. These systems are used by research professors and department administrators for conducting research and maintaining student information, including PII and grades.

- The student information included birth dates, addresses, and SSN.
- Some of the compromised systems were used by professors to conduct research for the Department of Energy
- Other infected systems involved technology research with potentially large economic payout.
- The research systems were not centrally backed up. Professors maintained individual backups on network shares and external media. Student data was centrally backed up.
- News started appearing on social media that there is a massive hacker attack on-going at the GRU. Rumors on social media said all computers at the University are infected and all University data has been breached. University employees who are not involved in the incident response are also attempting to respond to social media with their version of events – some helpful, some not. Local news media are calling GRU for information.
- Some faculty and staff are turning off their systems and calling their supervisor's offices asking for directions.

Discussion Questions:

1. What immediate steps should the University take? Who should be involved?
2. What are the issues that need to be considered/addressed? (privacy, ID theft, IP theft, breach notification requirements, etc.)
3. How should the rumors and news media be handled?
4. What information/instructions should be shared internally? Is there a communication plan in place to facilitate information sharing?
5. What long-term steps should the University take to protect its infrastructure/network?

BLUE GROUP – SECOND SCENARIO

Isolated Attack

A few hospital employees sign in to their local PCs only to find this message: "your systems and data have been encrypted and made unusable. You will receive our ransom demands shortly with payment instructions."

The IT department investigates the individual PCs in question. It also investigates broadly across the hospital network. The IT staff discovers "isolated" evidence of anomalies, including possible exfiltration of data and destruction of backups.

In the course of its investigation, IT finds a suspicious user account on its network with elevated privileges. It also finds that certain security software appears to have been disabled in the network.

What does management do?

GREEN GROUP – FIRST SCENARIO

False Breach

A cloud storage company is contacted by a hacker claiming he has obtained the company's user database and he will post it to the Internet if the company does not pay him $50,000. The hacker claims to have credentials for 10 million user accounts and includes a sample of the data including five user names and unencrypted passwords as proof.The cloud storage company tests the user names and passwords and they indeed work. The company cannot find any evidence on their systems that they have been hacked.

What are the issues at this point?

The company delays the hacker along for a few days, but getting frustrated, he posts to a well-known forum that he has hacked the cloud storage company and has obtained credentials for 10 million user accounts. Again a small sample of accounts is posted as proof. The hacker then ups his demand to $1,000,000.

An article is posted to an Internet news organization indicating that the cloud storage company has been breached. The company refuses to pay and releases a statement to the press saying they are not going to pay a ransom.

The hacker posts all 10 million accounts to the Internet. The company forces all users of its service to reset their passwords and offers a period of free service to the users as an apology. The extra customer service calls and the free service ends up costing the cloud company in excess of $2 million dollars.

The cloud storage company later analyzes the posted account data and finds noticeable discrepancies in the posted account data. It appears that the data may not have been from the cloud storage company at all, but from data breaches at other companies since the data includes information unique to those other breaches. A vast majority of the passwords that were supposedly for the cloud storage company do not work at all. The "hacker" appeared to have gathered accounts from the other data breaches and handpicked some samples that reused passwords as proof of the hack.

What if the company discovered hints that the hacker might be working for an investor at a competitor?

GREEN GROUP – SECOND SCENARIO

Ransom Hospital

A hospital desktop computer is infected with ransomware when the user clicks on an infected attachment. The desktop computer uses a network file share that contains medical charts and other health information for all currently admitted patients. The ransomware encrypts both the desktop computer and the admitted patient data.

After encrypting the data, the ransomware displays a ransom note on the desktop computer demanding payment. The IT help desk gets complaints that the admitted patient data file share is not working. Emergency manual protocols are invoked to continue patient care; the speed of admittance and discharge slows to a crawl.

IT examines the ransomware and determines that it also encrypted the admitted patient data. They also determine that they cannot recover the data without paying the ransom. Further, they find that this particular ransomware claims to have exfiltrated the encrypted data to the hackers. Other victims of this brand of ransomware claim that the hackers released their data on the Internet when they did not pay the ransom.

WHITE GROUP – FIRST SCENARIO

Dismissed Malware Alert

A retail company uses a third-party vendor to assist with order fulfillment. Company receives a message from vendor about a phishing email that was apparently sent from vendor's system. Vendor says company should investigate whether employees opened the attachment to the email, as it contained malware.

Company does a cursory investigation, but does not find anything. 10 days later, company receives a phishing email from the order-fulfillment vendor and begins to investigate. During this time, company starts to receive complaints about unfulfilled orders.

Company hires third-party forensics, who discover that numerous employees had opened the original malware, which arguably gave the attacker deep access into the company's network. Forensics finds a suspicious user account on its network with elevated privileges. It also finds that certain security software appears to have been disabled in the network.

Investigation also shows the company's managed services provider had sent an alert about the malware on a particular computer. At that time, IT scanned that computer with anti-virus but did not find anything, so they cleared the alert.

Six months prior the company hired a consulting firm to examine its org chart. That firm recommended that the company get rid of the CISO position and reorginize into operational units, which they did.

WHITE GROUP – SECOND SCENARIO

Not-So-Random Ransom

An insurance company is planning an annual meeting for its employees. As they prepare to attend, the employees interact with travel agent by email. Late Friday an email arrives from the travel agent to employee inboxes indicating that the final agenda update is attached.

The attachment did have a copy of the agenda in it, but it also included ransomware.

The ransomware encrypted data files found on infected computers, then demanded a ransom payment. Some employees report their local computers stopped functioning and are demanding ransom.

It is later determined that the email came from a compromised account at the travel agency. The attackers used DNS spoofing to redirect travel agent's web traffic to a look-alike travel reservation site to obtain their credentials. A number of the travel agents used the same password on the travel reservation site as their corporate password.

In the course of its investigation, the insurance company finds a suspicious user account on its network with elevated privileges. It also finds that certain security software appears to have been disabled in the network.

YELLOW GROUP – FIRST SCENARIO

Aggressive Researcher

A security research firm calls a medical laboratory to say that it has come into possession of a billing file belonging to the laboratory, containing patient names and Social Security numbers. The research firm claims that it obtained the file in numerous places scattered around an open peer-to-peer file-sharing network on the open Internet. The research firm emails a copy of the file to the laboratory. It requests a large fee to remediate the problem and remove copies of the file that are allegedly scattered all over the peer-to-peer network.

Investigation by the laboratory shows that the file is authentic and one employee did have unauthorized peer-to-peer technology loaded on a workstation, which could have enabled the research firm to come in to the workstation and take the billing file. But the investigation further shows that the file was not scattered anywhere. It had been located only on the workstation, and therefore the research firm must have taken it directly from the workstation without permission, in a deliberate, targeted attack. Investigation further shows that to find the file, a user of the peer-to-peer network required extraordinary expertise and persistence (like a professional security firm that is trying to position itself to earn a rich fee).

The research firm is well-known in the security community and the media. It receives government grants, as well as accolades from law enforcement groups around the country. The research firm is clearly not interested in identity theft or the commission of any kind of harm to patients.

YELLOW GROUP – SECOND SCENARIO

Insider's Alleged Revenge

An employee learns she will be terminated. Allegedly determined to get even, the employee downloads 4 gigabytes of data onto a flash drive and then purposely downloads ransomware onto the local computer and the network server.

The company's IT security assumes that this is a typical ransomware incident and focuses on recovering from the ransomware. Meanwhile the HR department dismisses the employee at the end of the week and the employee leaves with the flash drive.

IT security restores the server by the middle of the next week then looks at the former employee's computer. Security can tell that a sizeable amount of data was transferred from the company's network logs, but can't determine exactly what may have been downloaded. The former employee had access to proprietary product development information, the customer database, and data from the company's customers.

ORANGE GROUP – FIRST SCENARIO

Not the Typical Target

Hacker breaks into email network of a small financial institution. Hacker sends phishing emails to employees, asking to verify their employee ID. Email appears to be from employer.

Several employees respond with requested information.

Hacker then visits employer intranet site and clicks "change password."

Hacker is logged into employee email system and waits for email instructions to be delivered to inboxes.

Hacker takes that info and changes passwords, allowing access to employee's work HR system where paycheck direct deposit can be updated.

Hacker updates payment routing and account number for several employees.

Employer has safeguards to notify employees of any changes to direct deposit, but hacker is already in employee email accounts. Hacker deletes email notifications that the direct deposit information has changed.

Payroll funds are transmitted ultimately to foreign banks.

After payroll is run, twenty employees complain about not getting paid. An investigation ensues, and the FBI is called. By the time the foreign banks are contacted, the money has been withdrawn. The employees are from several different US states.

In the course of its investigation, the financial institution finds a suspicious user account on its network with elevated privileges. It also finds that certain security software appears to have been disabled in the network.

ORANGE GROUP – SECOND SCENARIO

Open-Source Uncertainty

A company that produces an open source product finds that the contents of its user discussion forum have been copied and posted online. Included in the data are the email addresses used to log into the forum and a limited amount of first and last names, since providing names is optional when creating an account. There are also hashes included in the data that appear to be user passwords.

The purported perpetrator also claims to possess all internal email records of the company, and promises to publish those as well.

What are the issues at this point?

Later it is discovered that the hashes do not represent passwords at all, but session information for users that were actively using the forum at the time of the of the data download. Forensic investigation reveals that the data was obtained through SQL injection.