Overview of the Duke Medicine Information Security Office

April 2013
What is the Duke Medicine Information Security Office?

• The Duke Medicine Information Security Office (ISO) is responsible for protecting information assets across all Duke Medicine entities, including:
  – Duke University Hospital
  – Durham Regional Hospital
  – Duke Raleigh Hospital
  – School of Medicine
  – School of Nursing
  – Research institutes
  – Ambulatory clinics
  – Health System corporate functions
  – Other related organizations.

• The ISO is lead by the Chief Information Security Officer (CISO), who reports to the DHTS CIO
  – The CISO has regulatory responsibilities as Duke Medicine's HIPAA Security Officer (includes all of DUHS, SoM, and SoN)

• The ISO is made up of a team of 12 security analysts
  – Additional positions being hired in FY13 to support new information security programs
Duke Medicine Information Security Office

Functional Areas

- **Cyber Defense and Response (CDR)**
  - Security Product Operations
  - Security Intelligence & Situational Awareness
  - Incident Monitoring, Alerting, & Response
  - Vulnerability Management & Pen Testing
  - Forensics

- **Security Policy, Awareness, Risk and Compliance (SPARC)**
  - Security Planning & Consulting
  - Security Policy Development
  - Risk Assessment
  - Awareness & Training
  - Compliance Monitoring

- **Security Engineering and Architecture**
  - Requirements Engineering
  - Network Architecture
  - Systems Architecture
  - Application Architecture
  - Lead security technology implementation projects
Background:

CURRENT THREAT AND REGULATORY LANDSCAPE
Data Breaches in the News:  
3.8 Million Tax Records Breached in S.C.

South Carolina official to resign over data breach, Nikki Haley announces

"The main question that I asked [the consultant] yesterday was, did we have a chance to do a better job? And we did."

S.C. Governor Nikki Haley

The head of South Carolina’s Department of Revenue will step down at the end of the year after a massive data breach exposed 3.6 million Social Security numbers, Gov. Nikki Haley said Tuesday.

Haley announced the resignation of department director Jim Etter during a press conference to unveil a third-party audit from security firm Mandiant that showed the state could have better protected personal financial data.

“The main question that I asked Mandiant yesterday was, did we have a chance to do a better job? And we did,” Haley said.
Data Breaches in the News

• **Healthcare organizations are a popular target…**
  – In 2011, 43% of data breaches were associated with the healthcare industry (government was #2 at 13.5%). Top 5 examples from 2012:
    • Utah Department of Health: 780,000 records
    • Emory Healthcare: 315,000 records
    • South Carolina Department of Health: 228,000 records
    • Howard University Hospital: 34,500 records
    • St. Joseph Health System: 31,800 records
  – Medical records, SSNs, credit card numbers, and other PHI can be monetized on the black market
  – Value of an individual medical record is over $50, vs. less than $1 for a credit card

• **…and Universities are as well.**
  – In 2011, 13% of breaches were associated with the Education sector, over 66 have been reported so far in 2012. Examples:
    • City College of San Francisco: 10+ years exposure of every network user
    • University of Tampa: 30,000 records
    • University of Nebraska: 654,000 records
    • UNC-Charlotte: 350,000 records
What Motivates Cyber Criminals?

• **Underground economy for stolen data**
  – Medical records, SSNs, credit card numbers, and other PHI can be monetized on the black market; used by criminals for identity theft and financial fraud
    • Stolen medical records have been valued at over $50 per record, vs. $1 or less for a social security number or credit card
    • Attackers want to gather this data in volume (thousands or millions of records at a time), but may sell individually

• **State-sponsored**
  – Well-funded, politically-motivated attacks against other governments or industry targets; goals may be espionage or disruption of critical infrastructure

• **Hacktivism**
  – Want to call attention to their social or political causes; often "anti-establishment" in nature

• **Curiosity and recreation**
  – Used to be the primary motivation for many attackers; still a motivator for those looking to prove themselves
What are Most Frequent Causes of Data Breaches Over the Past Year?

Source: DataLossDB.org
Data Breaches in Education
Over the Past Eight Years

By Type
Throughout the past eight years, hackings and malware have caused nearly a third of all educational data breaches.

- 219 Breaches: Hacking or Malware
- 198 Breaches: Unintended Disclosure
- 123 Breaches: Portable Device
- 52 Breaches: Physical Loss
- 47 Breaches: Stationary Device
- 21 Breaches: Insider
- 12 Breaches: Unknown or Other
- 1 Breach: Payment Card Fraud

Source: http://www.databreaches.net/wp-content/uploads/8-Years-Data-Breaches-In-Education-800.png
Some Perspectives...

- During 2012, Duke saw between 2M to 12M inbound attacks each month
  - Ebbs during the summer, with peaks during the holidays
- Phishing attempts, malware, and spam make over 80% of the email Duke mail servers process
  - Example from August 2012:

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Daily Average</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses, phishing, and other malware</td>
<td>93.6M</td>
<td>3.0M</td>
<td>80.6%</td>
</tr>
<tr>
<td>Spam (high or moderate rating)</td>
<td>4.8M</td>
<td>0.2M</td>
<td>4.1%</td>
</tr>
<tr>
<td>Legitimate email</td>
<td>17.8M</td>
<td>0.6M</td>
<td>15.3%</td>
</tr>
<tr>
<td>Total email</td>
<td>116.2M</td>
<td>3.8M</td>
<td>100.0%</td>
</tr>
</tbody>
</table>
Example of Phishing: Fake Email from Duke OIT

From: Duke OIT Service Desk <help@oit.duke.edu>
Subject: IMPORTANT NOTICE!!!
Date: April 9, 2012 7:44:32 AM EDT
To: Recipients <help@oit.duke.edu>

Your Duke Email account has been reported by students as fake. You may not be able to receive or send new messages. However, you might not be the only person to be victimized. To protect your account from sending spam, please go to the link below, fill the form and login again.

http://www.123contactform.com/form-3

Failure to do this will violate the University's Email Policy and Security. NOTE!!! You will be sent a password notification to your Email. For Security reasons.

DUKE OFFICE OF INFORMATION SERVICES
© 2012 Duke University, Durham, NC 27708 | (919) 660-7500

DATA CLASSIFICATION: RESTRICTED
More Examples of Phishing at Duke

Duke University <account@duke.edu>
To: undisclosed-recipients;;
New Message

ACCOUNT NOTIFICATION
You Have 1 New Message
Click Here To Read
Sincerely,
Duke University

Duke University Webmail © <support@duke.edu>
To: undisclosed-recipients;;
Reply-To: [email]
Duke University Webmail © <support@duke.edu>
Your Email Account has been Disabled:

Due to mismatch of your account details, your account has been Disabled.

Click here - Activate

© 2013 Duke University, Durham, NC 27708. All Rights Rese
INFORMATION SECURITY STRATEGY
Strategic Defense Model for Information Security

**Colonization**
Attacker maintains persistent access to compromised hosts and spreads

- Defend by detecting attacker’s presence and limiting their ability to spread
- Defend by controlling access to administrative privileges

**Infection**
Attacker bypasses perimeter defenses and compromises one or more one hosts

- Defend by decreasing the size of the attack surface and hardening hosts

**Disease**
Defenses fail to prevent the attacker from causing damage throughout the network

- Defend by disrupting the attacker’s command and control capabilities

Diagram based on SANS Top 20 Critical Security Controls
Strategic Defense Model for Information Security

Colonization
Attacker maintains persistent access to compromised hosts and spreads

Infection
Attacker bypasses perimeter defenses and compromises one or more hosts

Disease
Defenses fail to prevent the attacker from causing damage throughout the network

New Duke Medicine Information Security Strategy

Defend by detecting attacker’s presence and limiting their ability to spread

Defend by controlling access to administrative privileges

Defend by decreasing the size of the attack surface and hardening hosts

Defend by disrupting the attacker’s command and control capabilities

Diagram based on SANS Top 20 Critical Security Controls
### Guiding Principles for the Duke Medicine Information Security Strategy

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense-in-Depth</td>
<td>Defend throughout the environment, not just the perimeter</td>
</tr>
<tr>
<td>Balance</td>
<td>Optimize security, cost, and business enablement trade-offs</td>
</tr>
<tr>
<td>Simplify</td>
<td>Reduce complication and duplication of efforts</td>
</tr>
<tr>
<td>Respect</td>
<td>Value the privacy and academic freedom of our users</td>
</tr>
<tr>
<td>Partnership</td>
<td>Foster internal and external collaborations</td>
</tr>
<tr>
<td>Meaningful Metrics</td>
<td>Use evidence to optimize controls and risk decisions</td>
</tr>
</tbody>
</table>

DATA CLASSIFICATION: RESTRICTED
Information Security Strategy is Supported by People, Process, and Technology

### People and Process-Focus
- Risk Management
- Security Governance
- Security Policies, Procedures, and Standards
- Security Awareness
- Identity and Access Management
- Incident Response
- Data Governance
- Third Party Management
- Business Continuity Planning
- Secure Software Development Process

### Technology-Focus
- Data Loss Prevention (Symantec DLP)
- Encryption (Symantec PGP)
- Endpoint Management (IBM TEM)
- Firewalls (Cisco)
- Endpoint Protection (McAfee)
- Vulnerability Management (Tenable)
- Enterprise Governance, Risk, and Compliance
- Security Information and Event Management
- Mobile Device Management
- Intrusion Detection/Prevention
- Network Admission Control (NAC)
- Forensic tools
## Strategic Information Security Programs for FY13

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance, Risk, and Compliance</td>
<td>Policies, procedures, and standards to govern the program</td>
</tr>
<tr>
<td>Data Security</td>
<td>DLP, encryption, and governance processes to protect data</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>Manage and secure servers, desktops, and laptops</td>
</tr>
<tr>
<td>Network Security</td>
<td>Isolate network traffic based on security policies</td>
</tr>
<tr>
<td>Security Awareness</td>
<td>Educate the workforce on security threats and policies</td>
</tr>
</tbody>
</table>
## Strategic Information Security Programs for FY14

<table>
<thead>
<tr>
<th>Category</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Management</td>
<td>Identify, report, and remediate security vulnerabilities</td>
</tr>
<tr>
<td>Security Incident Management</td>
<td>Identify, report, and manage security incidents</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>Consistently manage of user identity and access controls</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>Minimize risks posed by personal mobile devices</td>
</tr>
<tr>
<td>Third Party Management</td>
<td>Ensure third party risks are understood and managed</td>
</tr>
</tbody>
</table>
## Strategic Information Security Programs for FY15

<table>
<thead>
<tr>
<th>Business Continuity Planning</th>
<th>Ensure all IT systems and processes can be recovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security</td>
<td>Implement secure software development practices</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Protect IT facilities from physical breaches</td>
</tr>
</tbody>
</table>
TIPS AND FAQS FOR RESEARCHERS
Think Before You Click!
- Practice skepticism when opening emails or web sites; do not open email attachments or click links unless they are from an expected/trusted source
- Be wary of social engineering attempts and phishing emails
- Don’t send sensitive Duke data or PHI to personal email accounts

Practice Good Password Management
- Use strong passwords or passphrases
- Use different passwords for different sites
- Never use a Duke password for a non-Duke site
- Never share your password!
- Example of a good passphrase: Bob and Tim are friends = B0b&T1mRFriendz!
- For help on password management, see: https://intranet.dm.duke.edu/dhts/iso/Shared%20Documents/Passwords%20Guidance.docx
What Can I Do? Staying Protected When Connected at Work, Home, and On the Go

• **Protect Your Computers**
  – Configured and manage systems per Duke Medicine IT standards and policies
  – Only install Duke-authorized software
  – Regularly apply security patches for operating systems and key applications
  – Maintain up-to-date anti-virus software
  – Use a password-protected screen lock when you’re not using your computer
  – **Encrypt all laptops!**

• **Protect Your Mobile Devices (Smartphones and Tablets)**
  – Set a PIN or password
  – Use automated controls to remotely wipe the device, or wipe the device after excessive failed login attempts
  – **Do not jailbreak or otherwise tamper with security settings!**

• **Protect Your Data**
  – Know what you have stored on mobile devices – especially USB flash drives!
  – Keep PHI and other sensitive data on a server – avoid making copies to a laptop or mobile device
Help! I've Been Hacked... What Now?

- The Duke Medicine Service Desk is the central point for initially reporting all security incidents
  - Web: http://helpdesk.dhts.duke.edu
  - E-mail: help-desk@mc.duke.edu
  - Phone: (919) 684-2243 or 1-800-684-2243

- The Service Desk will coordinate communications with the ISO and IT support resources for follow-up
  - The ISO will investigate the source and nature of the security incident
  - Your IT support team will address remediating any malware issues or rebuilding systems

- By the way: the same basic process applies for a lost or stolen laptop
Where Can I Find Security Policies and Standards?

• **Official Duke Medicine policy repository:**
  – http://marlowe.mc.duke.edu/accred/duhspol.nsf/fb44e3dd791dbda0852567910047d969?OpenView
  – Sorry for the horrible URL! Easier way to find them:
    • Go to http://intranet.dm.duke.edu/
    • Use the "Select a Policy" box in the upper right corner of the screen
  – Better system is coming!

• **Duke Medicine Information Security Standards:**
  – https://intranet.dm.duke.edu/dhts/iso/SitePages/Standards.aspx
What is DLP?

- The Duke Medicine Data Loss Prevention Program was designed to accomplish the following goals:
  - Create the ability for Duke Medicine to discover, monitor and protect data based on the Duke Data Classification Standard
  - Establish an inventory of sensitive data stored on servers across Duke Medicine
  - Assist in preventing accidental and intentional disclosures of sensitive electronic information by monitoring network and email traffic
  - Help identify poor data handling in current and historical business practices
  - Increase compliance with HIPAA and HITECH regulations, FISMA guidelines, NC ID Theft Protection Act, and PCI standards
  - Augments efforts to protect the Duke Medicine brand and reputation
How Does DLP Work?

• Communications leaving the Duke Medicine network and servers across Duke Medicine are scanned for specific types of "at risk" data:
  – Medical Record Numbers
  – Billing Account Numbers
  – Social Security Numbers
  – Credit Card Numbers

• Insecure transmissions of these data types will create an incident report that will be investigated by the ISO. For example:
  – Emailing sensitive data to personal email accounts
  – Emailing patients or research collaborators without using "$[Send Secure]"
  – FTP'ing files through unencrypted channels
  – Confirmed incidents are escalated to the appropriate Compliance Office (DUHS, SoM/SoN, PDC) for further action

• DLP Governance Committee was established to oversee DLP-related policies and execution of the program
  – Cross-functional group that meets at a minimum quarterly
  – Reviews and approves all changes to DLP policies
What is FISMA?

• **FISMA** is an acronym for Federal Information Security Management Act of 2002
  – “Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…”
    • Federal Information Security Management Act of 2002
    • Title III of the e-Government Act of 2002

• **FISMA provisions apply to Duke because we have a number of contracts and subcontracts where a government agency is the prime contract holder**
Duke’s Current FISMA Initiatives

• Create a FISMA-compliant Infrastructure as a Service (IaaS) model. The FISMA controls can be inherited for any systems that are served through the primary datacenters.
  – SSP for the Infrastructure has been completed and POA&M items have been documented
  – Next step is prioritization and remediation of POA&M items

• Centralizing FISMA administrative controls
  – Creation of a central FISMA training site and centralized tracking of training and certificates
  – Creation of a central process to ensure that all rosters of employees are accurate, updated with staff changes, and submitted to the agencies

• Centralization of all contract and related IT controls data
  – All data associated with contract and IT controls is being centralized on a single SharePoint site

• Implement Workstation Controls
  – Standardized “Research workstation”
  – Virtual desktop that eliminates the control issues associated with administrative rights.

• Centralize monitoring of key FISMA controls
  – Configuration Management – Tivoli Endpoint Manager project
  – Security Information Event Management (SIEM)
What is DICOM?

- **Digital Imaging & Communications in Medicine**
  - A standard for handling, storing, printing, and transmitting information in medical imaging.

- **Medical Images – pixel data and meta data**
  - PHI identifiers can be burned into the pixel data
  - Identifiers can be embedded into the over 3500 meta data tags
  - Deletion of all identifier tags will render the image useless
  - It may be impracticable in most cases to fully strip dates – strongly consider working with IRB to obtain consent/authorization to send embedded dates in the images
  - DICOM software may open holes in the firewall
  - Images may actually be stored with third party commercial vendors contracted by sponsors
Why and When Should I Engage the ISO?

• Why?
  – Provide guidance or training on policy, standards, or best practices
  – Conduct pre-purchase or existing software, hardware, or device risk assessment
  – Provide consultation on IT and security aspects critical workflows, architecture, secure innovative research
  – Investigate potential cyber threat such as hacking, identity theft, spam, phishing attempt

• When?
  – Before buying or installing any new, unapproved software, hardware, or storage device
  – Before you give access to Duke data to a non-Duke person, vendor, or organization
  – Before you engage a vendor to create a website, install hardware or software, or use their services
  – Before you clink on a link sent to you from an unverified source
  – ASAP when you realize that something may have gone wrong
    • Lost data, device, breach, inappropriate use of data by another
How Can I Contact the Information Security Team?

• **Duke Medicine Information Security Office**
  – Send Email to infosec@dm.duke.edu
  – Find us on the Intranet at http://infosec.dukemedicine.org/
  – In Service Now, Assignment Group "Security-DHTS"
  – Chief Information Security Officer: Chuck Kesler

• **Duke University IT Security Office (OIT)**
  – Send Email to security@duke.edu
  – On the web at http://security.duke.edu/
  – Chief Information Security Officer: Richard Biever