CYBER SECURITY WEBINAR
SEPTEMBER 16TH, 7- 8:15 PM ET

What You Need to Know to Effectively Protect Your ASC & Practice

Dan Chambers, Executive Director, Key Whitman Eye Center
Mark Johnson, President, Mednetworx
Brendan Gallagher, Information Systems Consultant, Medical Consulting Group
Skip Pleninger, President, Medical Insurance Division, Paris-Kirwan Associates, Inc.
Agenda

• Exposures & Trends – Skip Pleninger, President, Medical Insurance Division, Paris-Kirwan Associates
• Looking Ahead Market Conditions
• The Legal Landscape
• Case study – Dan Chambers, Executive Director, Key Whitman Eye Center
  Mark Johnson, President, Mednetworx
• Cybersecurity Everyday by Brendan Gallagher, Information Systems Consultant, Medical Consulting Group
• The Coverage – Skip Pleninger
• Q&A
Cyber Liability

Skip Pleninger, President, Medical Insurance Division, Paris-Kirwan Associates, Inc.

Disclaimer:
The material presented in this presentation is not intended to provide legal or other expert advice as to any of the subjects mentioned, but rather is presented for general information only. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Further, the insurance discussed is a product summary only. For actual terms and conditions of any insurance product, please refer to the policy. Coverage may not be available in all states.
CYBER SECURITY WEBINAR

Exposures & Trends
New Trends in Ransomware

• The overall trend is toward enterprise ransomware, which instead of attacking one machine or device, the attack spreads virally throughout the organization.

• Negotiating ransom is becoming less successful and generally ends up costing the victim more than simply paying the original ransom demand.

Targets:
• Network Credentials
• Email Credentials
• Banking Credentials
• Outlook contacts
• Emails

Best Practices:
• Implements endpoint monitoring
• Look for email and spam filtering improvements
• Train employees on best practices
In this corner, we have firewalls, encryption, antivirus software, etc. And in this corner, we have Dave!!
Responsible Party

- **55%** Employee
  - Often there is a combination of an employee mistake exploited by a non-vendor unrelated third party (i.e., a threat actor).
- **27%** Non-Vendor Unrelated Third Party
- **11%** Vendor
- **3%** Non-Vendor Related Third Party
- **2%** Unrelated Third Party
- **2%** Not Applicable

Source: BakerHostetler Data Security Incident Response Report 2019
**Data at Risk**

<table>
<thead>
<tr>
<th>Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>37%</td>
</tr>
<tr>
<td>Health Information</td>
<td>33%</td>
</tr>
<tr>
<td>Financial Account</td>
<td>19%</td>
</tr>
<tr>
<td>Driver's License or State ID</td>
<td>16%</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>15%</td>
</tr>
<tr>
<td>Payment Card</td>
<td>12%</td>
</tr>
<tr>
<td>Other &quot;Personal Information&quot;</td>
<td>4%</td>
</tr>
<tr>
<td>Passport</td>
<td>3%</td>
</tr>
<tr>
<td>Username and Password for Email or Online Account</td>
<td>3%</td>
</tr>
<tr>
<td>Student Information</td>
<td>2%</td>
</tr>
<tr>
<td>Taxpayer ID Number</td>
<td>2%</td>
</tr>
<tr>
<td>Biometric</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: BakerHostetler Data Security Incident Response Report 2019
Top 5 Security Breech Causes

1. **Phishing** 38%
2. **Network Intrusion** 32%
3. **Inadvertent Disclosure** 12%
4. **Stolen/Lost Device or Records** 8%
5. **System Misconfiguration** 5%

Source: BakerHostetler Data Security Incident Response Report 2020
W-2, Business Email Compromise & Phishing

- Scammers use emails from a target organization’s CEO, asking human resources and accounting departments for employee W-2 information.

- Scammers phish online payroll management account credentials used by corporate HR professionals.

- Scammers send emails pretending to have important Documents, or important new O365 mailbox audit log functionality

- Social Engineering
Incident Response Trends: Timeline

12 Days
Occurrence to Discovery

3 Days
Discovery to Containment

34 Days
Time to Complete Forensic Investigation

38 Days
Discovery to Notification

Average Forensic Investigation Cost
$58,034
All Incidents

$65,227
Average Network Intrusion

$350,576
Average of 20 Largest Network Intrusions Investigations

*This could lead to almost 3 months of business interruption in your organization*

Source: BakerHostetler Data Security Incident Response Report 2020
Who is being targeted?

- **23%** Healthcare (including Biotech & Pharma)
- **17%** Business & Professional Services (including Engineering & Transportation)
- **16%** Finance & Insurance
- **15%** Education
- **12%** Retail, Restaurant & Hospitality (including Media & Entertainment)
- **11%** Manufacturing
- **3%** Government
- **2%** Nonprofit
- **1%** Energy

Source: BakerHostetler Data Security Incident Response Report 2020
Security Checklist

1) Increase Email Security
   • Email is not a secure form of communication; every organization should use caution when sending or verifying sensitive information by email.

2) Implement Multi-factor Authentication (MFA)
   • MFA immediately increases your account security by requiring multiple forms of verification to prove your identity.

3) Maintain full data backups
   • A full data backup means the difference between a complete loss and a complete recovery after a ransomware attack.

4) Enable secure remote access
   • When remote access is allowed, your organization takes on additional risk.

5) Update your software regularly
   • Cybercriminals look for vulnerabilities that you can easily locate and prevent through regular software updates.
6) Use a password manager
   • Password managers help keep track of multiple passwords and are encrypted for maximum storage safety.

7) Scan for malicious software
   • Endpoint detection and response (EDR) tools readily identify, detect, and prevent advanced cyber threats.

8) Encrypt your data
   • Encryption is a process that renders data inaccessible to bad actors unless they possess the key required to access it. Non-encrypted data that is stolen is a large risk for your organization.

9) Set up a security awareness training program
   • 60% of claims are a result of human error. This can be avoided by creating a culture of cyber risk awareness that holds everyone accountable.

10) Purchase cyber insurance
    • Cyber insurance can prepare your organization for recovery in case of a breach.
Market Conditions
Looking Ahead

- Ransomware will remain the single biggest threat for all organizations
- The cyber insurance market will continue to harden throughout the year
- Supply chain attacks will be more common
- Government regulations and scrutiny will increase
- Criminal attacks will follow nation-state attacks
- Most cyber attacks will continue to be easily avoidable
The Legal Landscape
The Privacy “Patchwork”

- Federal & state laws govern the handling of PII/PHI
  - Laws covering SSNs / disposal of PII
  - Other federal and state regulations (e.g. FTC Act, Mass. Regs)

- HIPAA
  - Applies to Covered Entities and Business Associates
  - Preempted except where state law is “more stringent”

- State breach notification laws
- State medical information breach reporting laws
- International data protection regulations
State Laws

• All 50 States have Security Breach Notification Laws

• Laws vary between jurisdictions

• Varying levels of enforcement by state attorneys general

• Limited precedent
  – What does “access” mean?
  – What is a reasonable notice time?
The Key Whitman Case Study
Between 2019 and 2020 ransomware attacks rose by 62% worldwide and 158% in North America alone.¹

The level of attacks appears to be increasing, according to SonicWall. Ransomware volume jumped from 115.8 million attacks in 2021 Q1 to 188.9 million attacks in 2021 Q2.²

Within in U.S. Healthcare sector 40% of the cyber attacks since May, 2021 victims were in the Health or Medical Clinic sector [as apposed to Healthcare industry, Hospice or Elderly care, Hospital, or Medical University or Medical Research sectors.]³

¹ https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them
² https://threatpost.com/ransomware-volumes-record-highs-2021/168327/
90% of all attacks come from employee contacts

An Organization will fall victim to ransomware every 11 seconds

37% Co. hit; 32% paid Ransom; 65% encrypted data restored

FBI has now released a FLASH ALERT warning Health care Industry
  • Now a proliferation of HIVE RANSOMWARE
Anatomy of an attack

Now what?

Final Thoughts

CYBER SECURITY WEBINAR
Anatomy of an Attack

- Threat Actor (TA) Gains Access to your environment
  - Phishing and Spear Phishing E-mail
    - Look alike e-mails (banking etc.)
  - Web sites (nothing is free)
  - Employees (or ex-employees) selling credentials
  - Social Engineering
  - Constant attacks everyday everywhere Exploiting unpatched gear or zero day attacks

- TA investigates your environment
  - Looking for PHI and other monetizable data
  - Protected Health Information (PHI) is valuable
  - Protected Credit Information (PCI) is valuable

- TA Elevates their rights
  - Increasing their access to compromised accounts
  - Getting access to elevated accounts using tools

- The Attack
  - Destroy backups
  - Unleash encryption software
    - All script based
    - Ransom notes with codes
• You are responsible for your patient’s data regardless...
  • U.S. Department of Health and Human Services’ Office for Civil Rights (OCR)
    • OCR investigates all data breaches that impact more than 500 individuals
    • State attorneys generals

• Data Encryption
  • Assumption that if your data was encrypted by ransomware that data was exfiltrated unless there is credible evidence that it was not.

• Cyber Insurance/Business Continuity Insurance
  • Malpractice Insurance sometimes offers Cyber Insurance
  • Will policy pay the ransom?
  • Make sure that policy meets the needs of the Practice/ASC financially and otherwise.
Hardening your environment

Network
- Next Generation Firewalls/Intrusion Prevention System (NGFW/IPS)
- Endpoint Detection and Response (EDR) – more than Antivirus Protection
- Patching
- Security Event and Incident Management (SEIM) Monitored
- WIFI protection
- Encrypted Data

User ID’s & Passwords
- Multi Factor Authentication (MFA)
- Long complex passphrases for passwords or biometrics
- No administrative access at the end user level
- Limiting what end users can do (including doctors)

E-Mail
- E-mail – does everyone need it?
- E-mail filtering – more than spam filtering (AV, executables, ZIP files) and content

Backups
- (3-2-1) Multiple backups, Multiple Places, 1 Off-line (Air Gap)
- Encrypted Backups
• Business Continuance/Disaster Recovery (BCDR)
  • Contingency Plan for seeing patients in ANY situation when there is no access to EMR
  • List of Patients with Contact info for the upcoming day, week month with contact info
• Cyber Insurance/Business Interruption Insurance
  • Contact the insurance company to understand how to file a claim
    • Annual check of the insurance company vendors that are on their panel (Cyber mitigation vendors, cyber lawyers, cyber PR people)
    • Call the vendors and understand how they work
    • Decide on vendors
    • Having all of this information on paper, in your phone and in multiple places
• HIPPA Security Audits
  • They will find things to work on
  • It does not have to be expensive
• Policies for passwords, user ID’s etc.
• Personal device policies BYOD polices
• Cultural Change - Employee awareness (this is the weak link)
  • Getting employee and doctor buy in
Cybersecurity Everyday

Brendan Gallagher
Information Systems Consultant, Medical Consulting Group LLC
Cybersecurity Everyday

- Reasonable Controls
- Balanced Security
- Training and Awareness
- Communication
The #1 reason is a mistaken belief that current security is “good enough.”

- CompTIA's International Trends in Cybersecurity report

Nearly 68 percent of consumers would consider leaving their healthcare provider if it was hit by ransomware.
Defense in depth

- **Detect**
  - Use current endpoint security software with unified threat management - firewall, ad blocker, intrusion detection
  - Maintain your systems with current patches and updates
  - Inspect email and network traffic, including encrypted network traffic
  - Train staff to report unusual events or changes
Defense in depth

- Protect
  - Assess your physical, technical, and administrative controls - HIPAA
  - Maintain physical access controls
  - Use current technology in both software and hardware
  - Encrypt all data at rest and in transit wherever possible
  - Backup systems and data
  - Enforce strong passwords and use 2FA
Cybersecurity - Keys to Success

Defense in depth

• Recover
  – Test backup systems and recovery
  – Employ strong backup strategies (3 - 2 -1)
  – Plan for a disaster, breach, or emergency
Ransomware - Practical Tips and Tools

Ransomware Resources:

- Ransomware Simulator
  https://www.knowbe4.com/ransomware-simulator

- Breach Calculator
  https://eriskhub.com/mini-dbcc

- Vishing Example (Voice Phishing)
  https://www.youtube.com/watch?v=9njjpypnwl

Phishing Resources:

- KnowBe4 - Phish 100 users for free
  https://www.knowbe4.com/phishing-security-test-offer

- Google Phishing Trainer
  https://phishingquiz.withgoogle.com/

- King Phisher
  https://github.com/securestate/king-phisher
The Coverage

Skip Pleninger
President, Medical Insurance Division, Paris-Kirwan Associates, Inc.
Coverage Sections

Breach Response
- Legal Services
- Forensics
- Notification
- Credit Monitoring
- Public Relations

First-Party
- Extortion
- Interruption
- Restoration
- Cyber Crime*

Third-Party
- Cyber, Privacy and Network Security Liability
- Regulatory
- Payment Card
- Media Liability
First Party Coverage

Incident / Breach Response
- Legal/Breach Coach fees, forensics, notification costs, credit/identity monitoring, public relations, crisis communications, call center services etc.
  - Cyber Incident Response Expenses
  - Cyber Incident Response Coach / Legal Counsel

Data Restoration / Digital Asset
- Costs to restore or replace lost or damaged data or software
  - Digital Data
    - Does not include tangible property, or does it??
  - Digital Data Recovery Costs
    - Network Security Failure/Malicious Computer Act
First Party Coverage

Cyber Business Interruption

- Loss of profits and expenses from interruptions of insured’s systems; and with Contingent Business Interruption, adds losses from interruptions of others’ systems
  - Business Interruption Loss and Extra Expenses
  - Interruption in Service
  - Period or Restoration
  - Waiting Period
- Dependent Business Interruption Loss and Extra Expenses
- System Failure – Business Interruption (Non-Malicious Computer Act)
  - Human Error
  - Programming Error
  - Power failure of an electrical system controlled by and Insured, and not arising from Property Damage
- Dependent System Failure
First Party Coverage

Cyber / Network Extortion
• Payments to prevent digital destruction/impairment
  o Network Extortion Threat
  o Extortion Expenses
  o Coverage includes Ransomware
*also includes bitcoin and cryptocurrency*

Telecommunications Fraud
• Costs incurred as phone bill charges due to fraudulent calling
  – Telephone Fraud Financial Loss
  – Telephone System

Cyber Crime
• Computer Fraud: Third party accessing insured’s computers to take money
• Funds Transfer Fraud: Third party tricking a bank into transferring funds from insured’s account
• Social Engineering Fraud: Third party tricking an employee into transferring money
Third Party Coverages

Cyber, Privacy and Network Security Liability
- Failure to protect private or confidential information of others, and failure to prevent a cyber incident from impacting others’ systems
  - Network Security Failure
  - Protected Information
  - Privacy or Cyber Law

Payment Card Loss (PCI)
- Contractual liabilities owed as a result of a cyber incident
  - PCI Data Security Standards
  - Payment Card Loss
Third Party Coverages

Regulatory Defense, Fines and Penalties
- Defense for regulatory actions and coverage for fines and penalties
  - Privacy or cyber laws – includes state, federal and foreign
  - Consumer Redress Fund
  - Regulatory Fines

Media Liability
- Copyright and trademark infringement within scope of defined media content
  - Electronic, Social and Printed Media Liability
  - Media Incident
  - Media Content
Important Provisions & Reminders

Know your responsibilities as an Insured
- Reporting Security Incidents in a timely fashion
  - Engaging with your broker and carrier (s)
  - Reporting via email
  - Breach Hotlines

Breach Response Vendors
- Can we use our own counsel, forensics??
- Panel list review
  - Scheduling Preferred Counsel

Risk Management Portals and Additional Loss Mitigation Services
- Tabletop Exercises
- Security Awareness Training
Risk Management Services


- **NetDiligence** - [https://eriskhub.com/](https://eriskhub.com/)

- [https://chubbcyberindex.com](https://chubbcyberindex.com)

- Discounted Rates on services
Resources on Security Breach Information

- Ponemon Institute, LLC - [www.ponemon.org](http://www.ponemon.org)
- Privacy Law Blog - [https://www.bakerlaw.com/PrivacyDataProtection](https://www.bakerlaw.com/PrivacyDataProtection)
- Advisen Cyber FPN – [https://www.advisenltd.com/front-page-news/cyber-fpn-30-day-trial/](https://www.advisenltd.com/front-page-news/cyber-fpn-30-day-trial/)
Questions?

Presentation
Skip's Contact Info
Application
Checklist
Panelists Contact Information

Skip Pleninger
President
Paris Kirwan Associates Inc.
255 East Ave Suite 300
Rochester, NY 14604
Direct: 585-461-6427
Cell: 917-566-3056
Email: skipP@paris-kirwan.com
www.paris-kirwan.com

Dan Chambers
Executive Director
Key Whitman Eye Center
11442 N. Central Expwy
Dallas, TX 75243
Cell: 214-738-8954
Email: dan.chambers@keywhitman.com

Mark Johnson
President
MedNetworx
Office: 469-854-8451
Cell: 972-679-8364
Email: Mark.johnson@mednetworx.com

Brendan Gallagher
Information Systems Consultant
Medical Consulting Group, LLC
2808 S. Ingram Mill Road
Springfield, MO 65804
Office: 417-889-2040
Email: bgallagher@medcgroup.com
www.medcgroup.com