HALOCK®

FORESEEABLE THREAT INDEX REPORT

April 2018

In This Edition

- Distracting Healthcare
- CIS Adopts DoCRA
- Media Loss Deep Dive
- Why Some Breached Organizations Are Not Held Liable

HALOCK Security Labs

1834 Walden Office Sq.
Suite 200
Schaumburg, IL 60173

(847) 221-0200 (Office)
(800) 925-0559 (IR Hotline)

Risk Management
Compliance
Penetration Testing
Incident Response
Workforce
Security Engineering

Is Ransomware Distracting Healthcare?

FTI: Lost and Stolen Media Still Lead Breaches

Finding

Ransomware has seized the attention of Clinical Healthcare professionals, and for good reason. But the sector should not lose sight of their less-glamorous leader in information breaches; lost or stolen media and devices.

Threat Profile

The thought of healthcare providers losing access to critical systems and data though ransomware is frightening and attention-grabbing. But careful review of the HALOCK's Foreseeable Threat Index (FTI) shows that information security breaches in Clinical Healthcare have been caused most often by the loss or theft of media and devices … even while Ransomware catches up.

Since 2010, approximately 16.6% of all reported security incidents in Healthcare involved the loss or theft of portable media or devices. The threat breakdown includes the mishandling or mis-tracking of sensitive media and devices, loss from theft, loss within vehicles operated by the organization or its business partners, and use of media and devices in public locations.

The commonality of media-loss breaches is decreasing by both count and percentage of all causes, and the threat of ransomware continues to grow. This is a sign of progress. But if attention veers from less-glamorous causes for loss, avoidable breaches will persist.

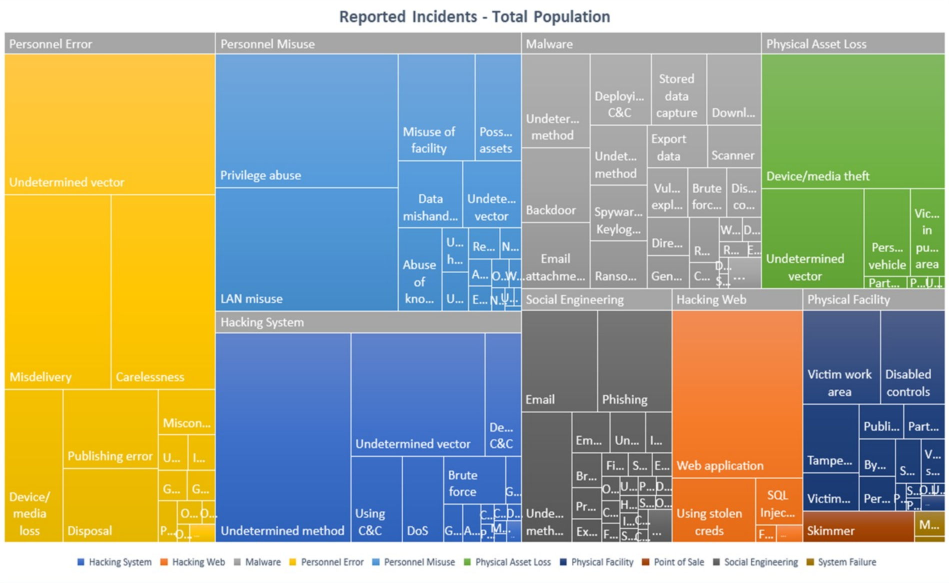
Foreseeable Threat Index

HALOCK Security Labs' FTI analyzes breach data from the public domain, and from HALOCK's incident response findings. The FTI provides an evidence-based approach for modeling threats and estimating their likelihood within individual industries.

HALOCK uses the FTI to help clients identify security controls that would prevent or detect the most common causes of incidents in their industry, and to prioritize risks based on the commonality of those breaches.

FTI can be used for risk analysis for any information security framework, includ-ing ISO 27000, NIST Special Publications and Cybersecurity Framework, PCI DSS, and CIS Controls.

Figure 1 - HALOCK Foreseeable Threat Index: Total Population



** The figure above is for demonstration purposes only, and does not reflect threat frequency for a particular industry or organization.*

Breakdown: Media Loss in Clinical Healthcare

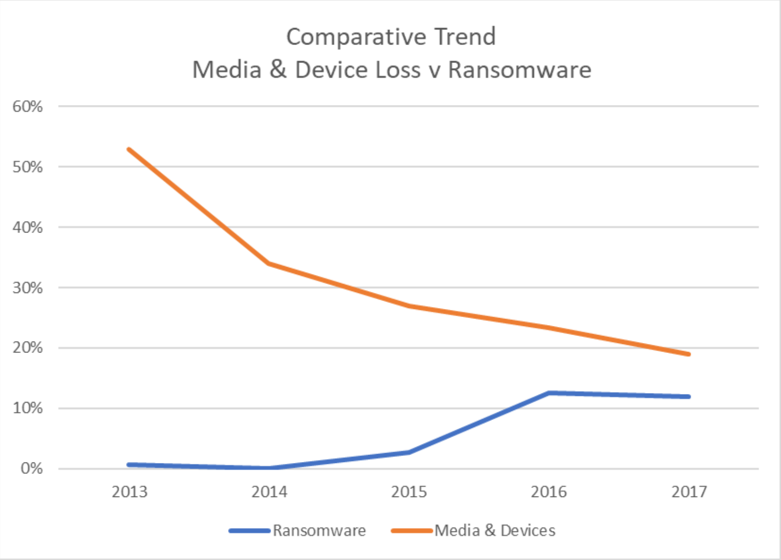
Findings

Theft and loss of media and devices containing sensitive information has been the leading cause of data security breaches in Clinical Healthcare both in aggregate (since 2010) and more recently in 2017. But the attention-grabbing Ransomware is gaining ground.

According to the Foreseeable Threat Index (FTI), technicians and end-users continue to store unencrypted information on media and devices which are susceptible to loss or theft. While information must be at some point unencrypted to be useful, especially in Clinical Healthcare, security controls that prevent mishandling are still presenting a major challenge.

Headlines about Ransomware appropriately grab our attention, but if Clinical Healthcare security focus is dedicated to Ransomware in spite of the continuing threats from non-secure media, breaches will continue to plague this sensitive but vital service.

Figure 2: Physical Asset Loss Breakdown in Clinical Healthcare



** From FTI Feb. 2018 Edition*

What Works for Others?

Loss of devices and media, including paper, laptops, smartphones is a challenge in large part because mobile assets are difficult to track; especially for "unconnected" devices such as backup tapes, paper, and USB drives. Primarily, the following safeguards should be considered for organizations whose risk assessments show that these threats create an intolerably high risk in their environments:

- Force-encrypt all media that may contain sensitive information. If assets are lost or stolen, the information may be protected when encrypted.
- Force-encrypt all files that store sensitive information to ensure that they are protected regardless of the media or devices they reside on.
- Prevent attachable storage devices from being connected to end-user systems that don't require them.
- Require that bulk unencrypted media, including paper that is being archived, are transported and stored by certified handlers and protected by lockable cases or bags.
- Force-encrypt and remotely manage all mobile devices that can attach to network resources, or that may foreseeably store sensitive information.

CIS Adopts DoCRA for Its Risk Assessment Method

Center for Internet Security (CIS), leaders in cybersecurity and community coordination, announced their adoption of the DoCRA Standard as the basis for their new risk assessment method, CIS RAM. At their launch of CIS Controls Version 7 on March 19, CIS announced their release of CIS RAM Version 1, a detailed, step-by-step guide for assessing cybersecurity risk using the DoCRA Standard (www.docra.org), which is available for **download.**

Organizations that use CIS Controls will have available to them a risk assessment method that fulfills the promise of a "reasonable" security standard by balancing the potential of harm to others against the burden of potentially costly or unwieldy safeguards. CIS' reputation for providing practical guidance required that the high-level principles and practices of the DoCRA Standard be supplemented by detailed instructions, templates, and examples. CIS RAM now goes beyond DoCRA to make those principles and practices simple to follow and implement. Attend the **CIS RAM Webinar on April 30, 2018** at 10:00AM EST.

Why Some Breached Organizations Are Not Held Liable

The University of Pittsburgh Medical Center was found not liable for damages by a lower court and appellate court after a data breach of their HR system. Hundreds of UPMC's employees reported identity theft and financial fraud after their personal and financial information was breached, and sued the medical center for failing to provide reasonable safeguards to protect the information. But the trial court and appellate court found that UPMC was not negligent after the courts applied a multi-factor "balancing test" that demonstrated to the bench that, in balance, the information was as protected as it could have been given the foreseeability of the breach, and the purpose of the medical center storing and using the data.

But these multi-factor balancing tests—at least in terms of data breaches—so far seem to fair worse for breached defendants than in the UPMC case. LifeLock was fined $100MM by the Federal Trade Commission for not providing "reasonable" security as evidenced by a risk assessment, even though they had a passing PCI DSS Report on Compliance and no reported security breaches. Target famously lost a motion to dismiss a lawsuit against them, thus permitting banks to sue them for damages suffered while replacing stolen credit cards. The judge in that case, Paul Magnuson, applied a balancing test to demonstrate that the risk to banks was foreseeable, despite the fact that the banks had no direct relationship with Target. And finally, LabMD had complained after FTC actions against them that it was not fair to be penalized after a breach of patient data because nobody told them explicitly what safeguards they were supposed to use to prevent the breach.

At first glance, these cases seem to be a hodge-podge of unrelated facts with unpredictable outcomes. Breaches with harm can lead to no liability, some cases with no breach and tough security certifications can create massive negligence. But courts and regulators are applying one concept to determine negligence; are foreseeable threats and impacts mitigated by safeguards that pose no more burden to the defendant than the risk itself creates?

Why Some Breached Organizations … (cont'd)

This concept of the "reasonable person" has vexed the legal and regulatory communities for decades. First encoded into a decision as the Learned Hand Rule (meaning that the burden of a safeguard should be less than or equal to the probability times the liability of harm, or "B <= P x L") this "reasonable person" has been part of regulatory and negligence law with varying tests to demonstrate its logic. The information security community knows these tests as "risk assessments" where likelihood and impact are estimated to determine whether risk is appropriate, and safeguards are evaluated to determine whether they are reasonable.

The Takeaway

Security breaches and regulatory violations may be difficult to prevent. But when organizations have a clear definition of the risks they protect against, and a clear demonstration that their safeguards are reasonable when compared to the risks, they have a strong claim for having provided due care. And because regulations use the "reasonable" standard for compliance, regulatory audits can be based on each organization's own "pass-fail" criteria, rather than waiting for the regulators to present their own terms.

What the Foreseeable Threat Index Tells Us

HALOCK's Foreseeable Threat Index provides our clients with an understanding of the prominence of breach-causing threats that occur in their industry. The index is a product of HALOCK's FTI Heuristic applied public data sources and HALOCK's collected intelligence on non-reported breaches. The FTI provides our clients with insight into what assets and functions within their organization may most likely cause harm. Because the FTI aligns those threats with security control standards, security practitioners can also ensure that their security and compliance programs focus on what matters most.

The Foreseeable Threat Index is not predictive, but it allows our clients to approach their security and compliance efforts using a "due care" model. When organizations think through the threats that cause the most reported breaches in their industry, and their security plans and controls address those threats to an appropriate degree, then they can demonstrate to interested parties that their priorities are appropriate for their risk.

About HALOCK

Established in 1996, HALOCK Security Labs is an information security professional services firm based in Schaumburg, IL. For more than 20 years, HALOCK has provided Purpose Driven Security services to help organizations achieve their mission and objectives through sound security practices. HALOCK uses their deep background in the legal and regulatory landscape, security technologies and standards, business governance, and data analytics to provide evidence-based security analysis and guidance to their clients.
(www.halock.com)

Foreseeable Threat Index Analysis Methodology

HALOCK makes no claim or representation that these data predict the causes for breaches in any one institution. To satisfy common regulations, information security standards, and due-care standards, organizations must evaluate their risk of these threats, and must plan and implement safeguards that reduce their risks to a reasonable level.