Why DLP is Critical to Protect Your Institution

March 30, 2022

Viviana Campanaro – CISSP

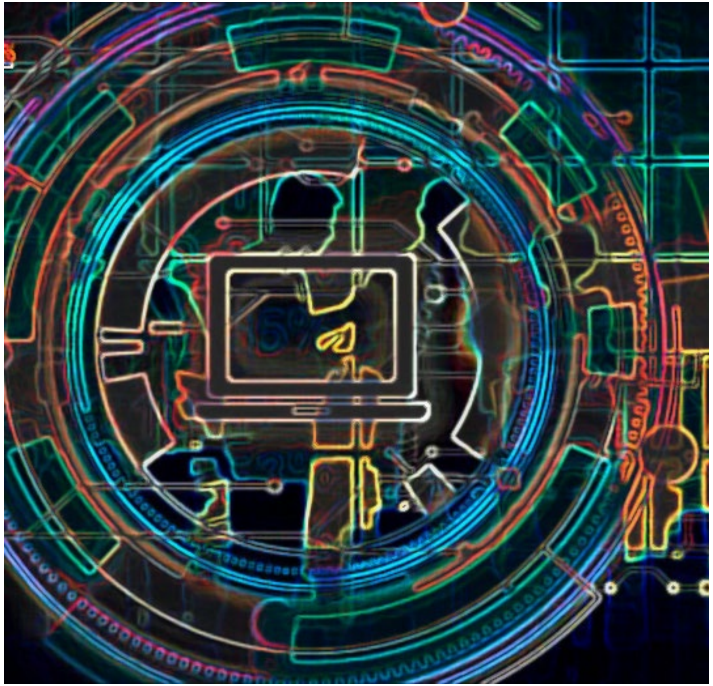
Security & GRC Solutions Specialist – Gladiator® at Jack Henry^{SM}

Scott Dale

Technical Product Manager – Gladiator at Jack Henry

What we'll cover

- Today's Threat Landscape
- What is DLP
- DLP Best Practices
- Key Takeaways

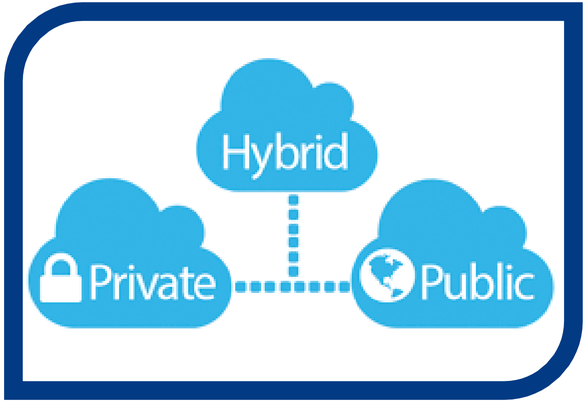


Today's Threat Landscape

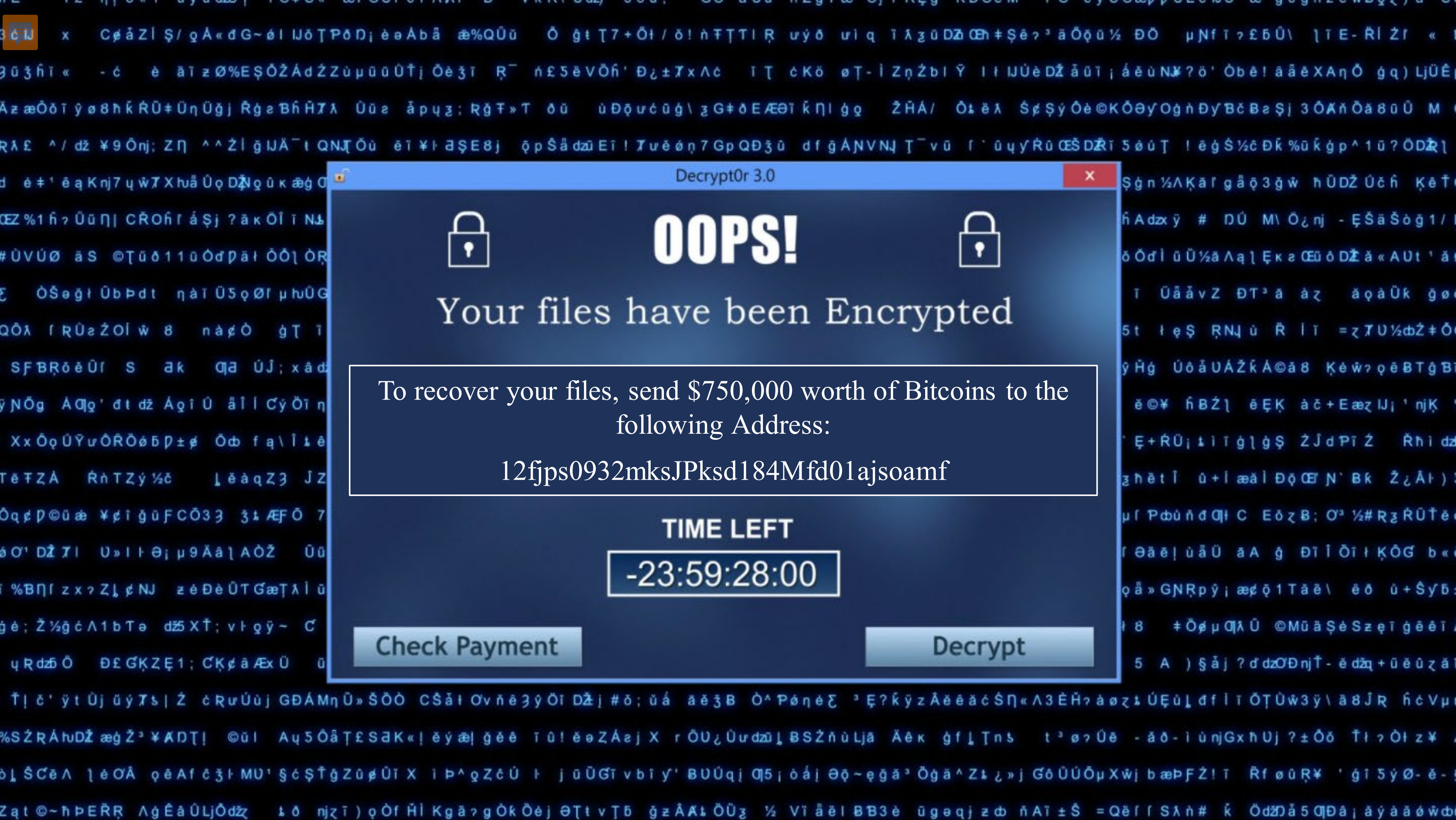
Sophisticated Threats

Geopolitical Conflict

Complex Environments



ZERO DAY



OOPS!

Your files have been Encrypted

To recover your files, send $750,000 worth of Bitcoins to the following Address:

12fjps0932mksJPksd184Mfd01ajsoamf

TIME LEFT

-23:59:28:00

Source: https://theguardian.com

Sanction Implications for US Financial Institutions

Global cyber threat level was raised to ELEVATED.

Overall cyber hygiene is the best protection.

Is your institution:

- Preparing now for a potential cyber-attack?
- Validating that your third-party service providers are meeting your information security standards?

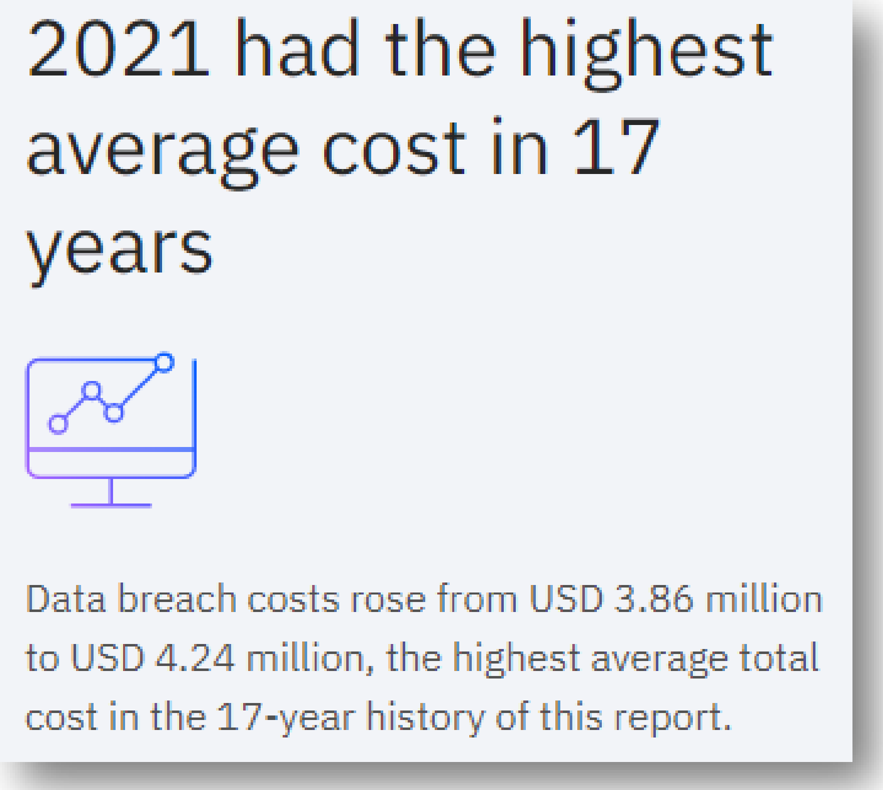
FS-ISAC

Executive Risk Report

18 March 2022 | EP - 02 - 2022

More Cyber Threats…

- Sanction-related Phishing
- Target US banking executives
- Vulnerability exploits
- Malware
- Data Exfiltration



2021 had the highest average cost in 17 years

Data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17-year history of this report.

Data breaches are expensive!

Source: https://www.ibm.com/security/data-breach

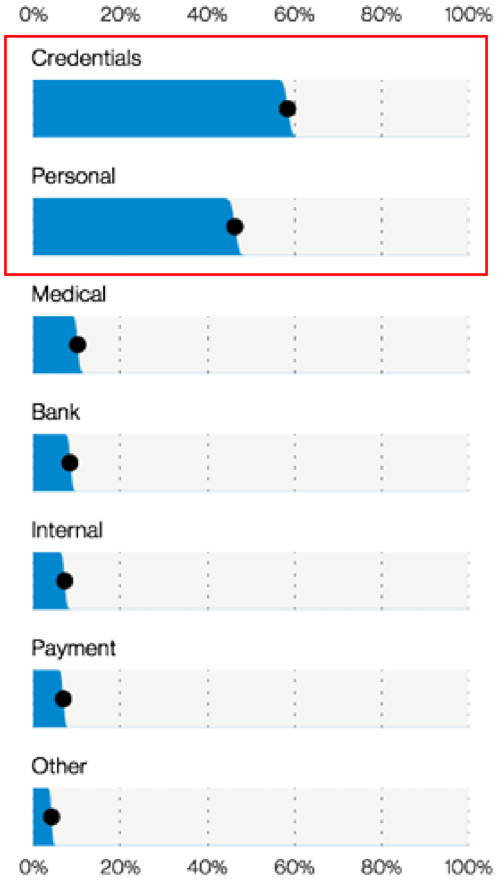
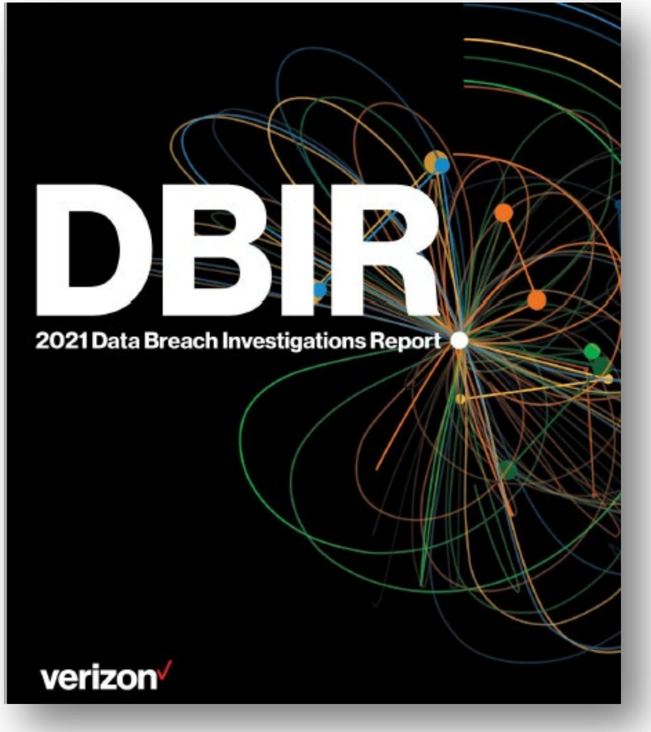


Figure 35. Top data varieties in breaches (n=4,552)



Source: 2021 Verizon Data Breach Investigations Report

Your Objective is to Ensure:

Data Security

- Confidentiality, Integrity

System Availability

- 24x7 access

Regulatory Compliance

How to Gain Total Visibility?

Modern-day security approach

- Integration of
  - People
  - Applied Threat Intelligence
  - SIEM/SOAR/SOC
  - Modern Security Technology

What is Data Loss Prevention (DLP)

“A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter.” - FFIEC

Data Loss Prevention (DLP) in Audits

Support and Delivery - Procedure 12 (FDIC InTREx Program)

Determine the adequacy of security monitoring for the network, critical systems and applications. Also determine whether sufficient controls are in place to protect against malware. Consider the following:

□ …

□ *Ability to detect and prevent the unauthorized removal of data from the network (e.g. data loss prevention)*

Source: FDIC, Information Technology Risk Examination Program

Data Loss Prevention (DLP) in Audits

FFIEC IT Examination Booklets

Information Security - II.C.9 Network Controls

Tools used to enforce and detect perimeter protection include… data loss prevention (DLP) systems.

Architecture, Infrastructure & Operations – IV.B Design Objectives

Management should include the following aspects in its architecture design:

- *Security and privacy throughout the entity's network (e.g., IAM controls and data loss prevention).*

Source: FFIEC, IT Examination Handbook InfoBase

What is Data Loss Prevention (DLP)

- Objective: Ensure data protection
- Identify sensitive information across your organization
- Prevent the unauthorized transfer of data outside your organization

Why Data Loss Prevention (DLP)

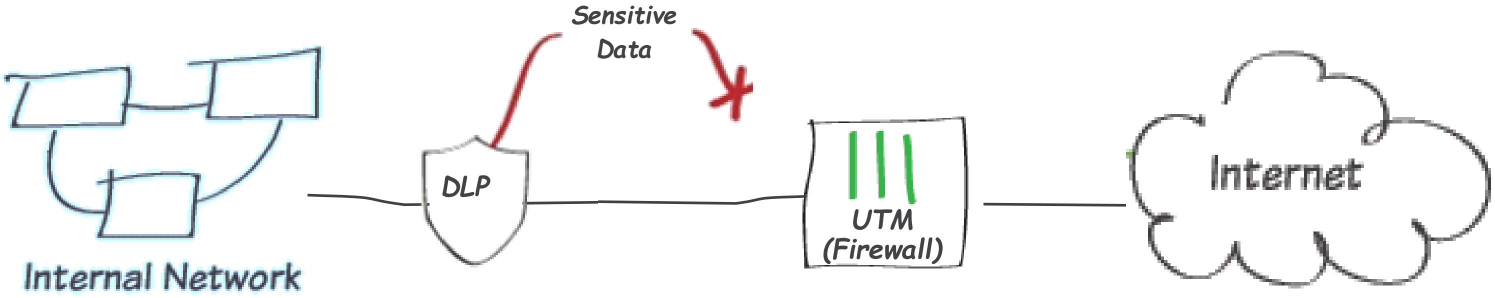
- Better Visibility
- Enforce Data Classification
- Protect Confidential Data
- Regulatory/Legal Compliance

Data Loss Prevention (DLP)

Network DLP	• Monitors data in motion • Implemented at network egress points (web/mail gateway, firewall)
Endpoint DLP	• Monitors data at rest • Data stored on workstations, servers, mobile devices • Implemented as endpoint agents
Cloud DLP	• Enforce endpoint DLP on cloud accounts • O365, Google, Azure, AWS

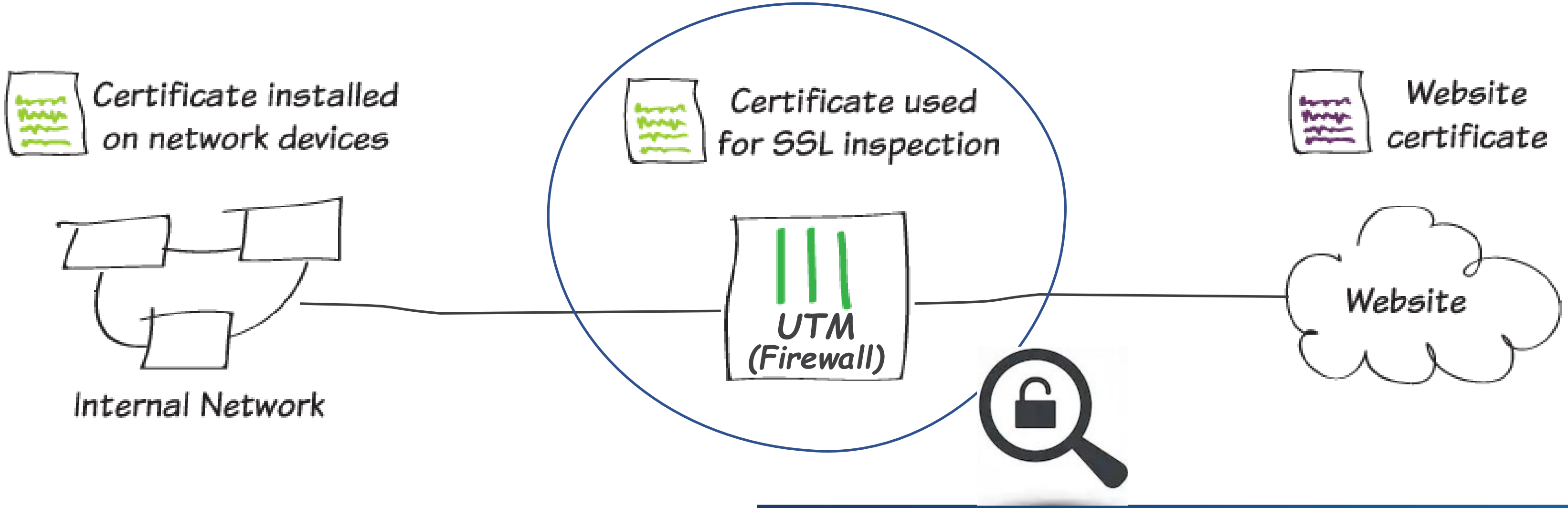
Data Loss Prevention (DLP)

- Keep sensitive information from leaving your network
- Data Leak Prevention (DLP) security profile
- Patterns of data leaving the network



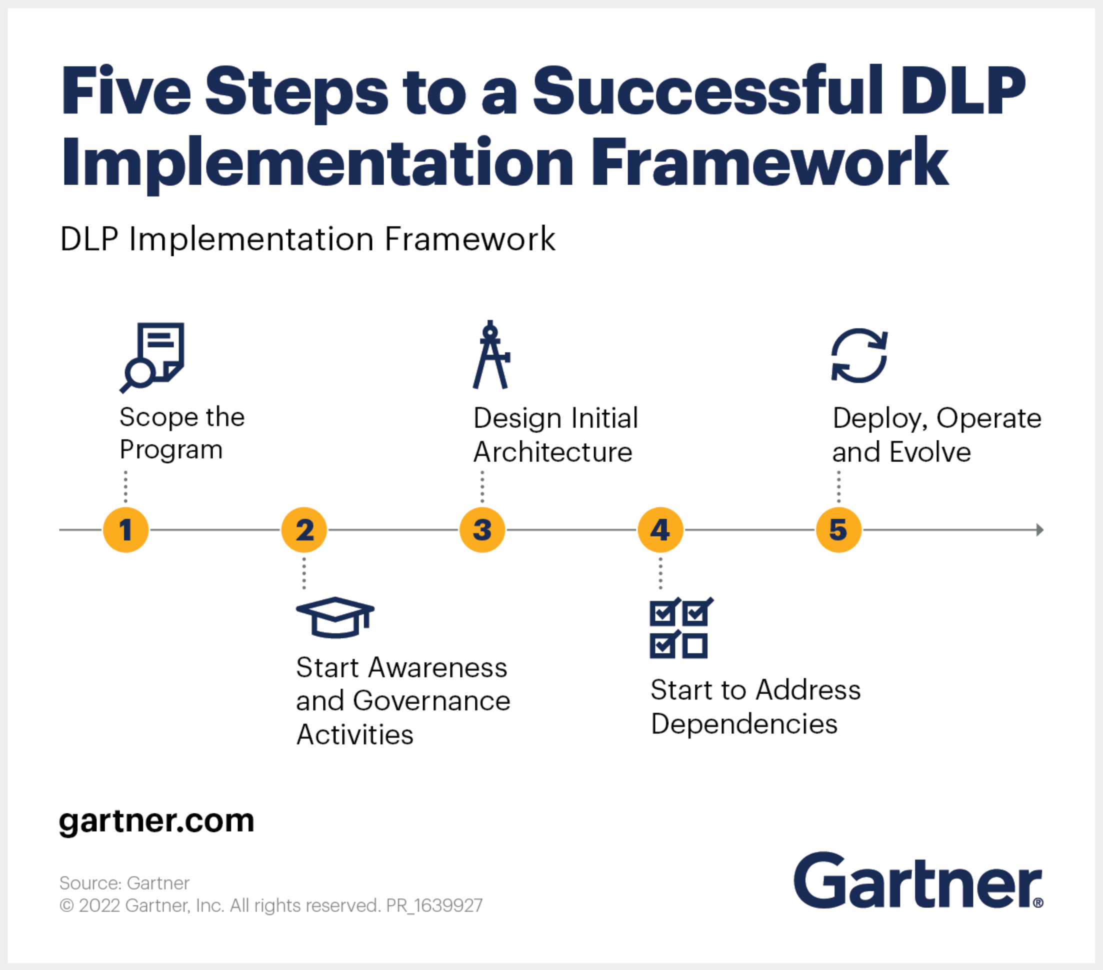
Encrypted Web Browsing (SSL-DPI)

- 85% of web traffic is encrypted
- Encrypted data cannot be inspected
- SSL – DPI (Secure Socket Layer – Deep Packet Inspection)


Certificate installed on network devices
Certificate used for SSL inspection
Website certificate
Internal Network
UTM (Firewall)
Website

DLP Best Practices

- Create a Data Inventory – Types, Location, Users
- Establish a Classification system – A common framework
- Perform a Data Assessment – Know what you're protecting
- Update your Policies – Data Handling, Incident Response
- Centralize the DLP Program – One Size Fits All (or should!)
- Implement in Phases – Prioritize based on risk
- Educate Employees – Data Handling Policies, Incident Reporting



Five Steps to a Successful DLP Implementation Framework

DLP Implementation Framework

1 Scope the Program

2 Start Awareness and Governance Activities

3 Design Initial Architecture

4 Start to Address Dependencies

5 Deploy, Operate and Evolve

gartner.com

Source: Gartner

Source: https://www.gartner.com/en/articles/build-a-successful-data-loss-prevention-program-in-5-steps

What to look for in DLP

Overall capabilities

- DLP Endpoint
- DLP Discovery
- DLP Network
- DLP Advanced Detection
- DLP Management System
- DLP Vendor Integrations
- Configuration Flexibility

Vendor/Service Provider

- Pricing Flexibility
- Understands Your Needs
- Technical Support
- Responsiveness
- Peer Reviews

Implementation

- Ease of Deployment
- End User Training
- API Integration
- 3rd Party Resources

https://www.gartner.com/reviews/market/enterprise-data-loss-prevention

Key Takeaways

- Inventory your data
- Know your risks
- Establish a proper framework for DLP
- Take time to research solutions
- Know the limits of DLP – It's not a silver bullet
- Consider 3rd party services to deploy and monitor

Jack Henry - Gladiator® Solutions

IT & Security Services
Total Protect™

Private Cloud Computing
HNS™

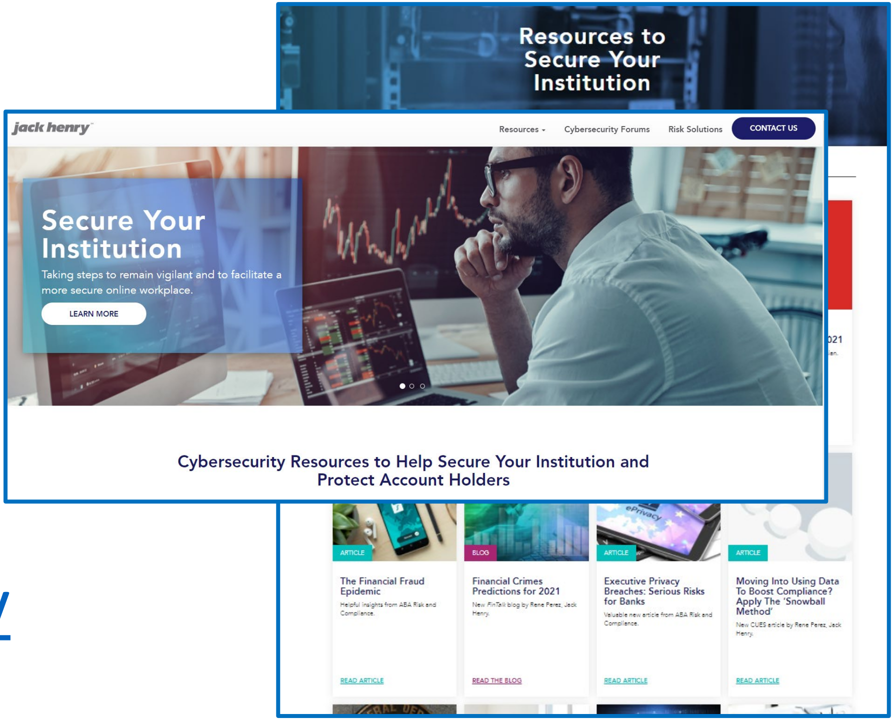
Backup & Recovery
Centurion™

Governance Risk & Compliance
GRC™

Cybersecurity Resource Center

- Webinars
- Cybersecurity Awareness Campaign
- Blogs penned by our SMEs
- Cybersecurity Forums
- Press Releases
- ICBA Preferred Service Provider
- And more…

jackhenry.com/cybersavvy



Resources to Secure Your Institution

Secure Your Institution

Taking steps to remain vigilant and to facilitate a more secure online workplace.

Cybersecurity Resources to Help Secure Your Institution and Protect Account Holders

The Financial Fraud Epidemic

Helpful insights from ABA Risk and Compliance.

Financial Crimes Predictions for 2021

New *FinTalk* blog by Rene Perez, Jack Henry.

Executive Privacy Breaches: Serious Risks for Banks

Valuable new article from ABA Risk and Compliance.

Moving Into Using Data To Boost Compliance? Apply The 'Snowball Method'

New CUES article by Rene Perez, Jack Henry.

Next in our Webinar Series

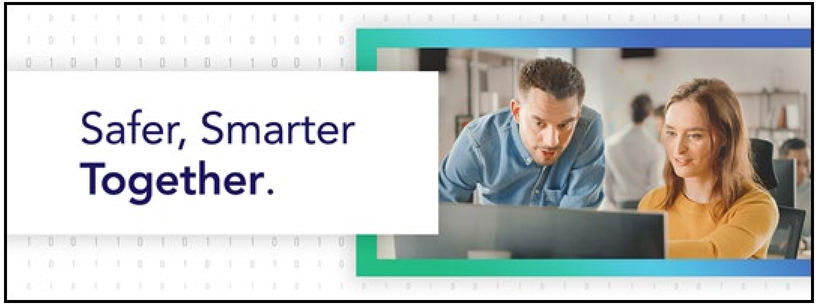
SIEM Part 3:
How Endpoint Detection and Response (EDR) Can Help Stop Breaches

Tuesday, May 24, 2022

2:00 p.m. CT

Register Now:

https://discover.jackhenry.com/cyber-security/new-webinars



Thank You!

Viviana Campanaro – CISSP

vcampanaro@jackhenry.com