HALOCK®

QUARTERLY EXECUTIVE SUMMARY

1st Quarter 2021

EXECUTIVE SUMMARY

With this inaugural edition of HALOCK's Quarterly Executive Summary we bring you significant events, trends, and movements from 2020 that will influence how you manage cybersecurity, risk, and compliance. Subsequent editions will highlight news from the previous quarter so our clients keep pace with – and ahead of – changes in our field.

Recent Security Incidents You Should Know About

Lorem Ipsum.

Threat Trends Globally and in Your Industry

Lorem Ipsum.

Recent Industry Reports and Updates

Lorem Ipsum.

Changing Laws

Lorem Ipsum. Lorem Ipsum.

Changing Standards

Lorem Ipsum. Lorem Ipsum. Lorem Ipsum. Lorem Ipsum.

Recent Industry Trends and Insights

Lorem Ipsum.

Industry Trends

Recent Security Incidents You Should Know About

BREACH	INCIDENT TYPE	DATE PUBLISHED	DETAILS
SolarWinds	Functional compromise at source code	December 2020	Read more
FireEye	Theft of Red Team tools	December 2020	Read more
University Clinic in Düsseldorf, Germany	Death of patient after ransomware attack	September 2020	Read more
Twitter	Account access/takeover	July 2020	Read more
Marriott	Employee at affiliate abused access and breached guest data.	February 2020	Read more

Threat Trends Globally and in Your Industry

INDUSTRY	FINDING	HIT INDEX
Clinical Healthcare	Is Ransomware Distracting Healthcare from Other Threats?	Lost and Stolen Media Still Lead Breaches
Education		
Manufacturing		
Professional Services		
Retail		
Information Technology Services		
Hospitality		

Recent Industry Reports and Updates

REPORT	INCIDENT TYPE	DATE PUBLISHED	DETAILS
Ponemon / IBM Annual Cost of a Data Breach Report	Sponsored, annual report about trends in breach costs at small or medium-sized organizations.	June 2020	Read more
Accenture Cyber Threatscape Report	A threat-focused report describes tactics, techniques and procedures of trending attacks.	October 2020	Read more
Ponemon Special Reports	Sponsored analysis of specific topics sponsored by Ponemon's clients.	Continuous	Read more
Verizon DBIR	Analysis of vectors, techniques, industries, and impacts of thousands of reported and unreported security incidents.	May 2020	Read more
NetDiligence Cyber Claims Study	Analysis of cyber breach claims from insurance carriers and brokers.	October 2020	Read more
ProofPoint State of the Phish	Analysis from the dataset developed within ProofPoint's email protection solutions.	January 2020	Read more

Changing Laws

LAW/REGULATION	DESCRIPTION	DATE PUBLISHED	DETAILS
HIPAA / HITECH HR 7898	DHHS Secretary may reduce breached organization's liabilities if they adhere to a security standard.	January 2021	Read more
CCPA	California's new privacy protection requirement. Requires companies to handle personal information according to consumer wishes.	July 2020	Read more
CPRA	California's update to CCPA privacy regulations. Grants further rights to consumers. Consumers now have a right to know what PI (private information) is *shared*, not just PI that is sold. Consumers can block *sharing* of information, and can block AI (artificial intelligence) from making decisions based on PI.	January 2023	Read more
CMMC	Department of Defense contractors must prove compliance with minimum security controls to retain contracts.	Three-year rollout plan in progress	Read more
Commonwealth of Pennsylvania v Earl Enterprises	State regulator defines reasonable security controls inan injunctive order against a breached restaurant chain. Their definition is consistent with DoCRA.	December 2020	Read more
Sedona Conference Commentary on a Reasonable Security Test	Influential think tank presents a definition of reasonable security controls for use by regulators, litigators, and the public.	September 2020 Public Comment Draft released.	Read more

Changing Standards

LAW/REGULATION	DESCRIPTION	DATE PUBLISHED	DETAILS
ISO 27701	Organizations can now certify their privacy program with ISO 27701. ISO 27701 certification is built onto an ISO 27001 ISMS. Both can be implemented at the same time, or ISO 27701 controls and processes can be added to an existing ISMS.	September 2019	Read more
NIST 800-53 Rev 5	NIST mainstay security standard issued by the federal government. Privacy is now a significant part of the controls set.	September 2020	Read more
CIS RAM 8.0	The Center for Internet Security, Inc. (CIS®)'s mainstay controls standard. Some controls have been combined. The current draft is now based on 18 controls, versus the 20 controls that have been the standard since its inception. There is deeper guidance language about each control.	~ April, 2021	Read more
PCI DSS Version 4.0	Mainstay security standard for securing payment card data is in development. Because controls are hard to always implemented as written, PCI DSS will be relying more on a risk basis for controls.	~ January, 2023	Read more

Recent Trends and Insights

TREND/INSIGHT	DESCRIPTION	ADDITIONAL INFORMATION
Limits of Industry Benchmarking	• Many reports are used for benchmarking budgets and breach costs, but their data widely varies (Verizon says $0.56/breached record. Ponemon says $245/breached record). • Our blog explains why these benchmarks are so different, and presents a better alternative for planning and budgeting your security program.	Read HALOCK Article
Sensitive Data Scanning	• Regulations increasingly require you to know where sensitive data is … and only use the data you are authorized to use. • This means you need to know where the data is so you can control it. • This is very hard to do. But it can be done as a service to reduce your effort and cost.	Read HALOCK Article

SERVICES/EVENTS/OTHER WE MAY WANT TO ANNOUNCE HERE

EVENTS/CONFERENCES

Lorem ipsum . Lorem ipsum . Lorem ipsum Lorem ipsum is the text we put here

CYBER SECURITY PROGRAMS

Lorem ipsum . Lorem ipsum . Lorem ipsum Lorem ipsum is the text we put here wh

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
844-570-4666

halock.com

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.

About the DoCRA Council

The DoCRA Council is a not-for-profit (501(C)(3)) organization that authors, maintains, and distributes standards and methods for analyzing and managing risk. The DoCRA Council is comprised of member organizations that require standards of practice in risk analysis and risk management, and who therefore have an interest in the methods used for analyzing risks and safeguards that reduce risk.