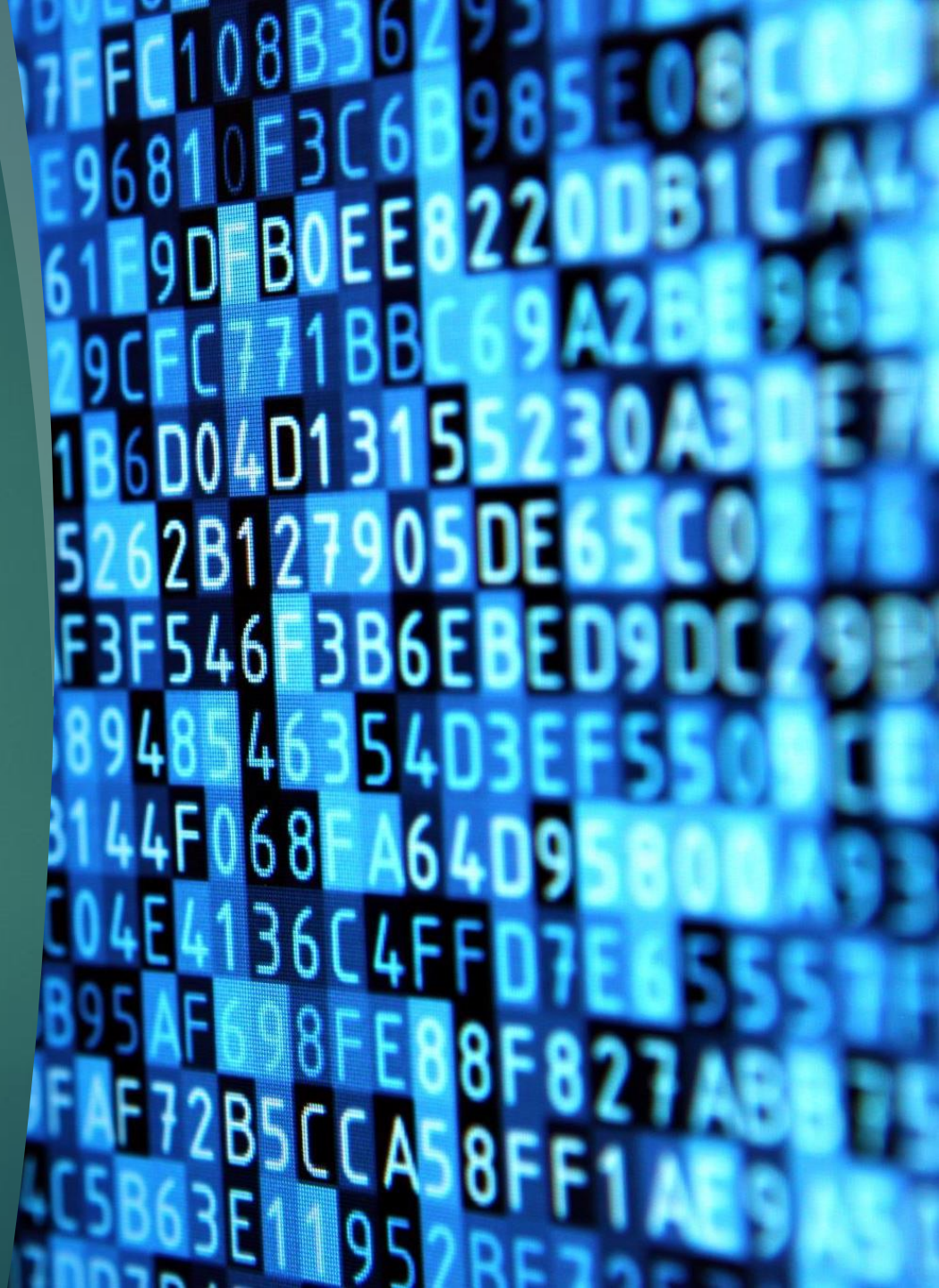
JR SECURITY CONSULTANTS

Global Security and
eCommerce
ISCPO Conference 2023

WWW.JRSECURITYCO.COM

Overview

- Cybercrime
- Six Pillars of eCommerce Data Security
- Data Protection Regulations
  - GDPR (International)
  - CCPA (Domestic)
- New/Changing Regulations
  - ICS2
- eCommerce Physical Security Trends



Cybercrime

- Cybercrime is the largest single threat to eCommerce security.
  - One-in-five eCommerce small retailers fall victim to data related breaches/fraud every year.
  - Of those, 60% will be forced to close within 6 months of the event.
  - Average global cost of a single breach is $3.62 Million USD. ($1M for small businesses to restore operations)
  - 3 out of 4 Small Businesses state that they do NOT have the personnel to address IT Security.
  - 54% of small businesses think they are NOT at risk and therefore do not have a cybersecurity plan in place.
  - 84% have no funds set aside to deal with data breaches/ransomware attacks.
  - Cyber-attack insurance

6 pillars of Security in eCommerce

Privacy

Integrity

Authentication

Non-repudiation

Confidentiality

Availability

The Basics of eCommerce Security

- **Privacy**

- Preventing unauthorized actors from reading, accessing, copying client/employee/company sensitive data.

The Basics of eCommerce Security

- **Integrity**

- Encrypting data both at rest and in transit. Granting the ability to detect changes and unauthorized access that occurs during transmittal or during storage.

The Basics of eCommerce Security

- **Authentication**
- Securely identifying signatories and servers via electronic signatures and handshakes. SFTP sites to ensure control over and authenticity of data transfers.
-

The Basics of eCommerce Security

- **Nonrepudiation**

  Provide and monitor end-to-end proof of each message's origin and receipt.

The Basics of eCommerce Security

- **Confidentiality**

  Protection against unauthorized disclosure of protected information. Requires in depth internal policies and procedures to educate and inform employees on how to handle and protect sensitive data.

The Basics of eCommerce Security

- **Availability**

  Provide delivery confirmation so data is not lost in transit. Provide protections that protect against data delays or removals.

General Data Protection Regulation (GDPR)

- General Data Protection Regulation (GDPR), is a legal framework that establishes guidelines for collecting and processing EU citizens' personal information.
- According to article 28 of the GDPR, a Data Protection Agreement (DPA) must be concluded when a company allows a service provider to process the personal data of its customers, users, or employees.
- A DPA is required any time a company processes individuals' personal data in the EU via a third-party service provider – even if the company itself doesn't have a legal entity in the EU.

GDPR Fine Analysis

- Lower-tier fines (for lower-level GDPR violations) of up to €10 million or **2%** of the company's total global turnover of the preceding fiscal year, whichever is **higher.**

- Higher-tier fines (for especially severe violations) of up to €20 million or **4%** of the company's total global turnover of the preceding fiscal year, whichever is **higher.**

GDPR Fines - Large Corporations

- **Top 5 Largest – 77 Fines over € 1,000,000**
  - Amazon Europe – 2021 – € 746,000,000 – Non-Compliance with general data protection principles
  - Meta Platforms – 2022 - € 405,000,000 - Non-Compliance with general data protection principles
  - Meta Platforms Ireland – 2023 - € 390,000,000 - Non-Compliance with general data protection principles
  - Meta Platforms Ireland – 2022 - € 265,000,000 – Insufficient technical and organizational measures to ensure information security
  - WhatsApp Ireland - 2021 - € 225,000,000 – Insufficient fulfillment of information obligations

GDPR Fines – Small Businesses

- **1,671 of 1,748 fines under € 1,000,000**
  - Private individuals, Police Officers, Banks, Hospitals, Universities, Government Agencies, Restaurants etc…

California Consumer Privacy Act (CCPA)

- **Took effect January 1, 2020** – Applies to:
  - Gross annual revenue in excess of $25 million.
  - Annually buy, receive for commercial purposes, sell or share for commercial purposes personal information of 50,000 or more California consumers, households or devices.
  - Derive 50% or more of their annual revenues from selling California consumers' personal information.
  - 15 other states have similar data protection regulations for their citizens.

CCPA Fines

- **What causes a fine?**
  - Failing to maintain a CCPA-compliant Privacy Policy
  - Failing to respond to consumers' requests under the CCPA rights
  - Failing to provide adequate notice when collecting personal information
  - Selling consumers' personal information without providing an opt-out
  - Discriminating against consumers who exercise their CCPA rights

CCPA Fines Analysis

- Maximum civil penalties of $7,500 for **intentional violations** of the CCPA brought by the State of California through the Attorney General's Office. Businesses will have only **30 days** to resolve the violation upon being notified by the Attorney General's office. Businesses will face financial penalties if they fail to resolve the violation within that time.
- Maximum civil penalties of $2,500 for **unintentional violations** brought by the State of California through the Attorney General's Office. Businesses will have only **30 days** to resolve the violation upon being notified by the Attorney General's office. Businesses will face financial penalties if they fail to resolve the violation within that time.
- **Consumers** can file private lawsuits for between **$100 to $750 damages** or for actual damages (whichever are higher) for each incident of breach of their unredacted and unencrypted data stored in a businesses' server. Companies will have only 30 days to resolve the violation upon being served a notice by the consumer or will face civil penalties.
- Fines are calculated on a **PER VIOLATION** basis

Import Control System 2 (ISC2)

- ICS2 introduces more efficient and effective EU customs security and safety capabilities that will:
- Increase protection of EU citizens and the internal market against security and safety threats;
- Allow EU Customs authorities to better identify high-risk consignments and intervene at the most appropriate point in supply chain;
- Support proportionate, targeted customs measures at the external borders in crisis response scenarios;
- Facilitate cross-border clearance for the legitimate trade;
- Simplify the exchange of information between Economic Operators (EOs) and EU Customs Authorities.

ICS2 Rationale

- The pre-arrival security and safety program will support effective risk-based customs controls while facilitating free flow of **legitimate trade** across the EU external borders. It represents the first line of defense in terms of protection of the EU internal market and the EU consumers. The new program will remodel the existing process in terms of IT, legal, customs risk management/controls and trade operational perspectives.
- The EU's new advance cargo information system ICS2 supports implementation of this new customs safety and security regulatory regime aimed to better protect single market and EU citizens. It will collect data about all goods entering the EU prior to their arrival. Economic Operators (EOs) will have to declare safety and security data to ICS2, through the Entry Summary Declaration (ENS).

ICS2 Non-Compliance

- Shipments being put on hold
- Rejection of shipment and possible intervention by customs authorities
- Fines and possible sanctions
- Disruption to a company's supply chain.

Physical Security - eCommerce

- According to the UPS survey of small- to mid-sized businesses, over half have lost more than $50,000 in the last year due to shipping incidents.
- Porch piracy: Two in five e-commerce merchants said that porch piracy has increasingly affected their business in 2022.
- Damaged shipments: Damaged items affected 36% of e-commerce consumers.
- Lost shipments: Over half (55%) of consumers have experienced package or item loss during the shipping and delivery process over the past two holiday seasons.
- Inventory delays: Twenty-eight (28%) of consumers were affected by late shipping and 19% experienced unfulfilled orders due to inventory challenges.
- Reverse logistics: Delays in claim resolution have resulted in business loss for merchants, according to the report. Two-thirds of e-commerce retailers have had to cover costs of product replacement, reshipment or refunds out of pocket prior to claim resolutions.

Physical Security

- In person audits of third-party providers and sub-contractors
- Training
- Corporate-level policies and procedures
- Accountability
- Communiation
- Vendor/Supplier Vetting Procedures