Cyber Security Awareness in the Printing Industries: Variable Data and Direct Mail Enterprises

Dr. Carl Blue & Dr. Charles Weiss
Graphic Communications
Clemson University

VDP and DM Markets

- The global variable data printing (VDP) market is expected to witness a compounded annual growth rate (CAGR) of 17.62% during the forecast period to reach a market size of US$29.255 billion by 2023, rising from US$11.050 billion in 2017.
- **In 2018, the average response rate of direct mail amounted to 4.9% for prospect lists and 9% for house lists. This is significantly higher than in 2017, with 2.9% and 5.1% respectively (ANA/DMA response rate report 2018).**
- According to MSP, a full-service direct mail marketing company near Pittsburgh, PA - 94% of marketing professionals across industries said personalized content is “important,” “very important,” or “extremely important” for meeting current marketing objectives.

Variable Data Printing – Direct Mail Marketing

- Many transactional print projects use multiple partners for complicated direct mail campaigns (one agent for inserts, one for letters, one for collation, etc.), which decreases control over the content and increases the risk of exposure.
- Print companies need assess their data processing activity, seek out expert advice, and develop a systematic approach and implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Cyber Security Awareness in the Printing Industries

- Status on VDP and DM industries
- Data Breaches – review some case studies where data associated to digital printing and direct mail services were compromised
- EU’s General Data Protection Regulation (GDPR) - how this affects data processors and data controllers
- Cyber Security – focus on some techniques promoted to protect the integrity of networks, programs and data from attack, damage or unauthorized access
- Recommendations for developing and incorporating data security practicum around variable data printing and direct mail services

Variable Data Printing – Direct Mail Marketing

- VDP and DM are a direct outgrowth of digital printing, which harnesses computer databases and digital print devices to enable the mass customization of documents via digital print technologies.
- Companies in the print industry can be classified as a data controller or data processors. A “data controller” determines the purposes and the means for which any personal data is to be processed (e.g. a bank) and a “data processor” processes that personal data on behalf of the controller (e.g. a print company).

What's at risk? Everything.

According to the 2019 Cybercrime Report by Herjavec Group, cybercrime damages are predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.
Data Breach at PIP Printing Company Leaks Thousands of Highly Sensitive Documents

- The company recently issued a statement saying it takes the security of its clients’ material very seriously.
- “We acted quickly to lock down access to our database and further secure our server and encryption,” PIP stated. “We immediately strengthened our security controls. We changed all passwords, took offline all computers that may have been affected, and we brought in forensic IT experts that are in the process of determining what data was involved.”

Data Breaches and Mailing Mistakes

- Large insurance carrier printed social security numbers that were visible through the window of the mailing envelopes. Paid $150,000 fines, had to pay for a year’s worth of credit monitoring for 33,000 individuals.
- A university sends out postcards reminding their 9,000 employees about annual benefit enrollment printed private information right below the address on the front of the cards. Workers eligible for a year’s worth of credit monitoring.

Data Breaches Will Soon Cost Companies in Europe

EU’s General Data Protection Regulation (GDPR)
- Firms operating in the EU will be subject to new regulations
- There are currently no overarching U.S. data-breach disclosure rules. Instead, companies must navigate a range of requirements across state legislation, in addition to U.S. Securities Exchange Commission’s breach disclosure guidelines, which apply only to publicly traded companies

EU’s General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) went into effect on May 25, 2018. If your organization handles personal data of EU individuals, you must comply or face fines of up to €20m, or 4% of annual global turnover.
1. Understanding “Data Controller” and “Data Processor”
2. Records of Processing Activities
3. Individuals’ Rights
4. Security and Privacy by Design
5. Network Consolidation
Two Approaches to Mitigating Risk

- One is “hardening” the system to ensure that they are not exposed to the outside and thus more vulnerable to attack.
- In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one.
- Two, implementing user controls through print management solutions that provide protections such as user authentication, secure print and auditing technologies.

Comprehensive Solutions In a Competitive Industry

- Undertaking an exhaustive third-party audit of security practices.
- Assuring customers they’re qualified to create, access, store, and exchange highly sensitive, regulated data, such as PHI (Protected health Information).
- Abiding by HIPAA (Health Insurance Portability and Accountability Act) data security guidelines.
- Implementing and meeting control objectives and specifications in a variety of security categories ranging from physical plant and environmental asset management.

Cyber Security Awareness – Model

- Identify Threats – External and internal cyber security threats
- Identify Vulnerabilities – Develop inventories of onboard systems with direct and indirect communication links (Consequences, capabilities, and limitations)
- Risk Analysis – Determine likelihood of external threats, inappropriate use, and impact of being exploited
- Develop protection and detection measures – Reduce vulnerabilities, reduce impact
- Establish contingency plans – Develop a response-plan(s) to reduce the impact of threats
- Respond to Cyber Security Incidents – Assess impact of effectiveness of the response plan, and reassess threats and vulnerabilities

Threats and Mitigation

- Email
  - Phishing (Baiting, Pretexting, Phishing) – Legitimate in appearance
  - Malware – Malicious attachments – Viruses, Denial of Service (DoS), Ransomware
  - Spear Fishing – focused attack on an individual or organization
  - SPAM – 14.5 billion emails globally per day which is 45% of all email
- Cloud Computing
- Passwords Security
- Employee Training

Email Usage

This data set shows that, as of 2018, there are about 124.5 billion business emails sent and received each day, while there are about 111.1 billion consumer emails sent and received each day.

Email Mitigation

- Use strong, unique passwords
- Don’t reuse passwords
- Avoid using personal information
- Use two-factor authentication
- Keep software up-to-date
- Be cautious with attachments
- Avoid clicking links in suspicious emails
- Be aware of social engineering tactics
- Use anti-virus software
- Report suspicious activity

May 15, 2019 - www.campaignmonitor.com/blog/email-marketing/2019/05/shocking-truth-about-how-many-emails-sent/
2018 President’s Conference Keynotes Announced

Dr. Carl Blue
cnblue@clemson.edu
200 K Godfrey Hall

Presentation Resources

- Infographic resource available (drag and drop): http://www.united-mail.com/direct-mail-resources/infographics.php
- Data Breach and Mailing Mistakes: https://mailingsystemstechnology.com/article-3642-Data-Breaches-and-Mailing-Mistakes.html
- EU Council Data Protection Regulation: 5 Implications for the Print Industry: https://www.unica.eu/services/insights/jpg
- Data Breach at PIP Printing Company Leaks Thousands of Highly Sensitive Documents: https://www.xerox.ca/en-ca/services/insights/gdpr
- Data Breach Will Cost Companies in Europe: https://www.unica.eu/articles/data-breaches-will-cost-companies-in-europe-1311186400

Printed by Printing Industries of America