Cybersecurity Awareness In the Printing Industries: Variable Data and Direct Mail Enterprises

Dr. Carl Blue and Dr. Charles Weiss

Keywords: cybersecurity, data security awareness, variable data, direct mail

Abstract

The variable data printing (VDP), and direct mail (DM) markets are witnessing impressive growth due to its high adoption rate and rise in digitalization. This continuing trend toward designing and delivering individualized mail and targeted printed materials is dependent on accessing computer databases of personal, demographic, and geographical information. This increasing reliance on computer databases by these data controllers and data processors heightens the need for comprehensive approaches in expanding data security awareness and mitigating risk. In VDP and DM operations where production controls were relatively insecure in the past, there is now a heightened need for developing approaches to mitigating risk and implementing comprehensive contingency plans for responding to data breaches in these highly competitive industries. Furthermore, our educational centers associated with the diversity of graphics industries are encouraged to implement curriculum on security awareness and training for secure data management. Academic programs that ignore these dangers of not implementing security awareness are putting their students' reputations and future employers at a disadvantage. The goal of this report is to bring cybersecurity awareness to the graphics industry and those in academia on the increasing need for knowledge of the risks involved in keeping data secure.

This paper has been developed by two faculty members collaborating on data security in the variable data printing and direct mail services. This work includes a shared focus on developing curriculum and educating students for careers in the graphics industry. It also includes working with industry partners in enhancing their variable data printing and direct mail services. This collaboration links the scholarly pursuits of those connected to the graphics industry with those in the information security of an increasing need for awareness of the risks involved in

Clemson University

keeping data secure. With the increase of data breaches across the spectrum of industries and organizations that compile and use data, a heightened awareness of the risks involved in keeping data secure is the goal of this paper.

Variable Data Printing and Direct Mail Marketing

Variable Data Printing (VDP) and Direct Mail Marketing (DM) are a direct outgrowth of digital printing. These print endeavors harness computer databases and digital print devices to enable the mass customization of documents via digital print technologies [10], [9]. The global variable data printing (VDP) market is anticipated to witness a compound 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 [12]. In 2018, the average response rate of direct mail amounted to 4.9% for prospect lists and 9% for house lists. This response rate is significantly higher than in 2017, with 2.9% and 5.1%, respectively (ANA/DMA response rate report 2018) [8]. 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 [2].

Additionally, these print industry enterprises can be classified as data controllers 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) [14]. One of the reasons controlling the data gets complicated is that many transactional print projects use multiple partners for complicated direct mail campaigns (one agent for inserts, one for letters, one for collation, one for mailing etc.), which decreases control over the content and increases the risk of exposure [7]. Print companies need to 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 [7].

What’s at risk? Everything. All too common, headlines like this Forbes’ article from February 20, 2020, stated, “*MGM Resorts Data Breach Exposes Personal Information Of 10.6 Million Guests*,” Personal data details of some 10.6 million guests were reportedly posted on a hacker forum.[1] 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, and predicts that a business will fall victim to a ransomware attack every 11 seconds by 2021 [4].

Data Breaches in the Printing Industries

A recent data breach at PIP Printing Company leaked thousands of highly sensitive documents. In 2017, an online security breach at a national printing chain leaked thousands of confidential documents raising the possibility that private information could end up in the wrong hands. The leak at PIP Printing, which has more than 400 locations in 13 countries, went on for four months before it was repaired. The breach exposed 400 GB of highly sensitive data, and the documents included emails revealing credit card and social security numbers, legal filings such as depositions, subpoenas and labor lawsuits, and extensive medical records [5]. The company 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." [11]

Digital printing trends for designing and producing individualized and targeted messaging products increase the risk for data breaches, even on applications like direct mail marketing, where production controls have been relatively loose in the past. In a direct mail example, a large insurance carrier printed social security numbers visible through the window of the mailing envelopes. Paid $150,000 fines and had to pay for a year's worth of credit monitoring for 33,000 individuals. In another mailing incident, a university sent out individualized postcards reminding their 9,000 employees about annual benefits enrollment and printed private information right below the address on the front of the cards. Workers were eligible for a year's worth of credit monitoring. [6]

Other factors increase exposure for data breaches, such as improperly disposed or stolen computers or drives - programmers or management take work home with them. Once it leaves the company's environment (often without authorization), sensitive data can be at risk. Operations that ignore the risk are putting their companies, their reputations, and their jobs on the line. Guarding against accidental breaches should be a focus for document operations. Security awareness should probably be heightened in all document centers. [6]

European Union's General Data Protection Regulation (GDPR)

Firms operating in the European Union (EU) are now subject to new regulations, as data breaches can result in fines for companies in Europe. The EU General Data Protection Regulation (GDPR) went into effect on May 25, 2018. If an organization handles personal data of EU individuals, they must comply or face fines of up to €20m, or 4% of annual global turnover. There are several implications for the Print Industry as follows:

- *Understanding who is the "Data Controller" and "Data Processor."*
  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). May need to appoint a data protection officer (DPO).
- *Records of Processing Activities*
  Under the new regulation, both data controllers and data processors are required to maintain records of data processing activities and make those records available to supervisory authorities if requested.
- *Individuals' Rights*
  Close oversight and personal data tracking are essential to comply with GDPR's strengthened rights for individuals to have their data erased or, if appropriate, the processing of the data stopped. Print companies, as data processors, may be required to assist data controllers with access requests.
- *Security and Privacy by Design*
  The new GDPR reporting window for data breach notifications is 72 hours.
- *Network Consolidation*
  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.

The GDPR's requirements could result in an increase in business for larger OEMs. Customers may seek the safety of a one-stop-shop that manages sub-processors across all geographic locations and provides infrastructure, security, and automated reporting within a controlled environment [7].

Presently there are currently no overarching US data-breach disclosure rules. Instead, companies must navigate a range of requirements across state legislation, in addition to the US Securities Exchange Commission's breach disclosure guidelines, which apply only to publicly traded companies [7].

Approaches to Mitigating Risk

There are a variety of approaches for 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 more significant when a system performs more functions; in principle, a single-function system is more secure than a multipurpose one. Another approach is implementing user controls through print management solutions that provide protections such as user authentication, secure print, and auditing technologies. [3]

They are undertaking an exhaustive third-party audit of security practices. Assuring customers, they're qualified to create access and store and exchange highly sensitive, regulated data, such as PHI (Protected Health Information), and abide by HIPAA (the 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. [3]

Cyber Security Awareness Model

The model created as part of the guidelines used on board ships and for shipping can also be applied to VDP and DM, and is very relevant to the cybersecurity threats. The model works like SWOT analysis to identify an organization's strengths, weaknesses, opportunities, and threats in a competitive environment. [16].

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

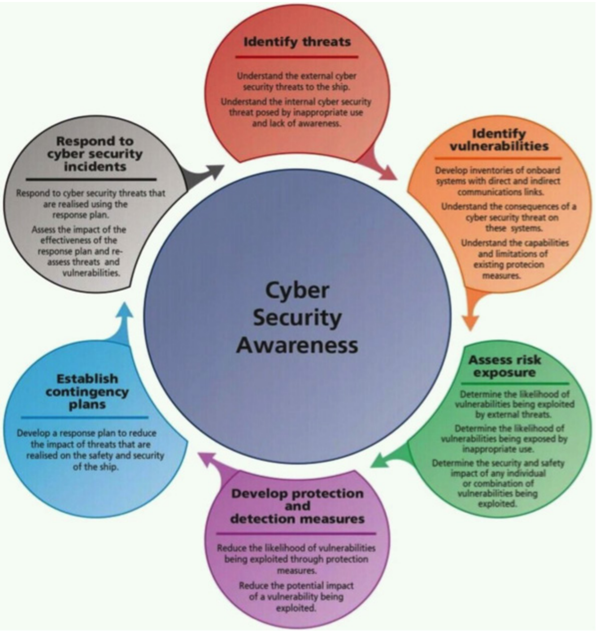
Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
Cyber Security Awareness

Figure 1. *Cyber Security Awareness Model [17]*

Closing

Printing Industries of America, 2018 President's Conference Keynotes, David Mauro of All Covered IT Services from Konica Minolta shared best practices and methods to secure and manage your systems as well as how to handle compliance and notice requirements in the event of a data breach. David Mauro surmised "Why IT Matters," stating, "Now more than ever, there is a potential liability that exposes client when a data breach happens." He continued over the past two years has seen the highest cases for data breaches and lost records, and the trend is increasing in occurrence. He stressed that IT security and meeting compliance stands should be the focus for many organizations [13]

When an enterprise's employees are cybersecurity aware, they understand cyber threats. Cyber-attacks will have a potential impact on their business and the steps required to reduce risk and prevent cyber-crime infiltration of their online workspace. [15]

Cybersecurity awareness education is shown to minimize security deficiencies and improve compliance. A survey was conducted that collected 415 employee responses from various companies with security policies in place. The findings indicated that employee's non-compliance was caused by factors including security anxiety, and lax in security education and security visibility [15].

Going forward, the promotion of further research into cybersecurity awareness and training in the printing industries and graphic communications education programs is a desirable and applicable approach toward safeguarding compliance and reducing risk by providing education for students and training for employees a culture of security awareness.

References

[1] Cimpanu, C., 2020. *Exclusive: Details Of 10.6 Million MGM Hotel Guests Posted on A Hacking Forum.* [online] www.zdnet.com. Available at: <https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/> [Accessed 28 May 2020].

[2] Frankenberry, A., 2017. *Why Direct Mail Marketers Love Variable Data Printing.* [online] www.msp-pgh.com. Available at: <https://www.msp-pgh.com/variable-data-printing/> [Accessed 28 May 2020].

[3] Gansler, J. and Binnendijk, H., 2019. *Working Paper, Information Assurance: Trends in Vulnerabilities, Threats, And Technologies.* [online] /www.hsdl.org. Available at: <https://www.hsdl.org/c/> [Accessed 28 May 2020].

[4] Morgan, S., 2017. *2017 Cybercrime Report.* [online] cybersecurityventures.com. Available at: <https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf> [Accessed 28 May 2020].

[5] O'Hara, M., 2017. *Data Breach at PIP Printing Company Leaks Thousands of Highly Sensitive Documents.* [online] www.nbcnews.com. Available at: <https://www.nbcnews.com/news/us-news/data-breach-pip-printing-company-leaks-thousands-highly-sensitive-documents-n718886> [Accessed 28 May 2020].

[6] Porter, M., 2012. *Data Breaches And Mailing Mistakes* [online] mailingsystemstechnology.com. Available at: <https://mailingsystemstechnology.com/article-3642-Data-Breaches-and-Mailing-Mistakes.html> [Accessed 28 May 2020].

[7] Trentmann, N., 2017. *Data Breaches Will Soon Cost Companies In Europe.* [online] www.wsj.com. Available at: <https://www.wsj.com/articles/data-breaches-will-soon-cost-companies-in-europe-1511386000> [Accessed 28 May 2020].

[8] Vojinovic, I., 2019. *Direct Mail Statistics That Will Have You Running to The Post Office.* [online] www.smallbizgenius.net. Available at: <https://www.smallbizgenius.net/by-the-numbers/direct-mail-statistics/#gref> [Accessed 28 May 2020].

[9] (N/A), 2011. *Saving Mailing Costs with Variable Data Printing.* [online] http://ondemandexpo.com/. Available at: <http://www.ondemandexpo.com/on-demand-newsletter/saving-mailing-costs-with-variable-data-printing> [Accessed 28 May 2020].

[10] (N/A), 2012. *ABC's of VDP, A Variable Data Printing Basics Guide.* [online] www.efi.com. Available at: <https://www.efi.com/library/efi/documents/327/efi_fiery_abc_vdp_wp_en_us.pdf> [Accessed 28 May 2020].

[11] (N/A), 2017. *PIP Responds to News Regarding Data Breach.* [online] www.globenewswire.com. Available at: <https://globenewswire.com/news-release/2017/02/12/916216/0/en/PIP-Responds-to-News-Regarding-Data-Breach.html> [Accessed 28 May 2020].

[12] (N/A), 2017. *Variable Data Printing Market - Industry Trends, Opportunities and Forecasts To 2023.* [online] www.researchandmarkets.com. Available at: <https://www.researchandmarkets.com/reports/4451951/variable-data-printing-market-industry-trends> [Accessed 28 May 2020].

[13] (N/A), 2018. *2018 President's Conference Keynotes Announced.* [online] www.printing.org. Available at: <https://www.printing.org/press-room/2018-presidents-conference-keynotes-announced-0> [Accessed 28 May 2020].

[14] (N/A), 2018. *EU General Data Protection Regulation: 5 Implications for The Print Industry.* [online] www.xerox.ca. Available at: <https://www.xerox.ca/en-ca/services/insights/gdpr> [Accessed 28 May 2020].

[15] (N/A), 2018. *The Importance of Cyber Security Awareness.* [online] www.ogl.co.uk. Available at: <https://www.ogl.co.uk/the-importance-of-cyber-security-awareness> [Accessed 28 May 2020].

[16] (N/A), 2018. *The Guidelines on Cyber Security Aboard Ships.* [online] Available at: < https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> [Accessed 01 August 2020].

[17] (N/A), 2016. *Cyber Security Threats in the Shipping Industry.* [online] Available at: < https://soldecom.com/cyber-security-threats-in-the-shipping-industry/ > [Accessed 01 August 2020].