Sherita-Tara (Tara) KI**SSOO**N, MSc, MBA, CISSP, CISA, LLQP, is a multi-certified I.T. Risk & Security Leader with twenty-five years of technology experience, twenty years of experience in the financial services industry focusing on technology, cybersecurity, governance, risk and compliance, along with professional and community volunteering. Tara actively volunteers at ISC2 and St. Patrick's Parish in Markham and attained her Enhanced Police Information Check (E-PIC), Vulnerable Sector Check, Biometrics, Bail Verification, NEXUS and maintain medical records for identity verification, to volunteer/work in high-risk communities, and cross borders as a trusted traveller. Details are located @ www.it-rs.org.

Abstract:

When an organization is attacked through a breach of information security controls, the law requires the organization to notify individuals that their personal identifiable information (PII) has been exposed. It has a privacy risk and may cause significant harm to the individual.

When accessed data is transferred to unauthorized individuals for the purpose of fostering criminal activity, the personal identifiable data elements become extremely important. Criminals harvest and sell this information on areas of the internet known as the dark/deep web, to propagate further criminal activity. This is the primary reason why funding secure measures in organizations are important to protect organizations from data and privacy breaches which result in this type of impact to citizens.

This article will explain the concept of identity takeover through the use of a concrete example. This article will share a strategic framework that could be used by various stakeholders involved in the implementation of cybersecurity measures to safeguard sensitive data and leverages a data centric focus on the evolution of cyber-attacks. Specific security measures are important and should be implemented appropriately to alleviate cybersecurity threats. This article will provide a case study utilizing the cybersecurity risk management framework to show that it provides the elements necessary to create a defensible way of assessing risk, with the implementation of adequate internal controls to ensure the protection of data and privacy as required by law.

This article will touch on topics such as digital privacy and data protection. Specifically, digital privacy is the practice of protecting information, which is accessible on the internet, and facilitates mechanisms of using this information in a secure manner, without leaking or compromising the information. Digital privacy is inclusive of protection of an individual's data which is created, accessed, collected and disclosed through electronic means. Throughout the years, use of the internet has transformed the way an individual manages their information, with rapid accessibility by unknown third parties.

Industry reports have shown that there is an increase in the number of reported data breaches where an individual's information is exposed and used in a fraudulent manner. Therefore, data protection laws are important to provide a legal framework to manage online privacy.

These laws vary across different countries with the enforcement process dependant on the jurisdiction. One of the most important data protection legislations enacted to date is the General Data Protection Regulation (GDPR). Currently, there are more than one hundred and twenty countries that have enacted legislation to secure the protection of data and privacy.

The European Union's (EU) General Data Protection Regulation, implemented in May 2018, brought data protection into the public and is considered a landmark privacy law with the introduction of new rights for individuals, such as the Right to be Forgotten and the Right to Portability.

The European Union's (EU) General Data Protection Regulation (GDPR) encompasses ten key areas that apply to data protection. Within the scope of this regulation, there are three specific requirements which were taken into account, 1) personal data breaches, 2) privacy by design, and 3) data protection impact assessment. Within the law, the requirements to evaluate the data security risk with the implementation of appropriate controls is evident. "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.

In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage." [1]

The information provided in this article will give the necessary data to show that the cybersecurity decision-making process can be clearly integrated with risk management methodologies. As most cost benefit analysis usually underestimates either the cost required by an organization to adequately control the privacy of a user's personal information or the total cost resulting from a data breach.

"FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook[2]

Facebook, Inc. will pay a record-breaking $5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy, to settle Federal Trade Commission charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information."

[1] European Union Agency for Networks and Information Security, Octave v2.0, viewed May 2020, https://www.enisa.europa.eu.

[2] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Viewed March 2024, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Identity Takeover: From the Lens of the Victim

This topic has been the center of many important discussions by various executives across all industries globally. Business executives recognize the need to implement secure measures to address various privacy laws, regulations and industry standards to protect their organization from external and internal attacks (i.e., unauthorized users, malicious code, network/application layer attacks).

Data protection laws were put in place to protect personal identifiable information (PII) of a citizen in response to technological and societal changes. The law requires organizations to notify individuals that their personal identifiable information (PII) has been exposed at the time an executive uncovers that their organization has experienced a breach of information security controls: "1) compromised electronic information systems, 2) theft, 3) transmission errors, 4) social engineering, 5) phishing, 6) failure to secure, and 7) accident publication of personal information. It has a privacy risk and may cause significant harm to the individual". [3]

Headlines like these are crippling and cause significant risks to organizations:

"Met Police Officers at Risk After Serious Data Breach. London's Metropolitan Police Service is investigating a serious data breach that may have exposed names, ranks and photographs for potentially all 47,000 personnel. One concern with the breach is that undercover officers' identities may have been exposed."[4]

With the evolution of ransomware-as-a-service, this type of cybercriminal activity is intertwined with organized crime making this a global multi-million dollar criminal business. Although, there are special law enforcement task forces focused on this type of activity, it may take decades to dismantle, takedown and arrest cybercriminals.

A recent example of a successful FBI Operation by Team "Duck Hunt":

"Qakbot Malware Disrupted in International Cyber Takedown: Qakbot Malware Infected More Than 700,000 Victim Computers, Facilitated Ransomware Deployments, and Caused Hundreds of Millions of Dollars in Damage."

"Cybercriminals who rely on malware like Qakbot to steal private data from innocent victims have been reminded today that they do not operate outside the bounds of the law," said Attorney General Merrick B. Garland.

Together with our international partners, the Justice Department has hacked Qakbot's infrastructure, launched an aggressive campaign to uninstall the malware from victim computers in the United States and around the world, and seized $8.6 million in extorted funds." [5]

---

[3] PIPA Breach Report 2022, viewed September 2023, https://oipc.ab.ca/wp-content/uploads/2022/07/PIPA-Breach-Report-2022.pdf.

[4] Met Police Officers at Risk After Serious Data Breach, viewed September 2023, https://www.bankinfosecurity.com/met-police-officers-at-risk-after-serious-data-breach-a-22947.

[5] Qakbot Malware Disrupted in International Cyber Takedown, viewed September 2023, https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown.

At the time accessed data is transferred to unauthorized individuals for the purpose of fostering criminal activity, the personal identifiable data elements become extremely important. Criminals harvest and sell this information on areas of the internet known as the dark/deep web, to propagate further criminal activity.

It is within this realm of the internet that data is repurposed to create identification for sale and reuse. Although the identification is used by a fraudster, the information used to create the ID (i.e. passport, drivers license, citizenship card, credit/debit card) is real and attached to a known individual within society. Creation of these types of identifications allow fraudsters to impersonate the individual and use their personal identified information to conduct criminal activity. In most cases, this is known as identity fraud and the rightful owner of the personal identifiable information is unaware that their information is being repurposed for reuse to support criminal activity. Usually, the individual eventually becomes aware through banking, credit, government or employment relationships. At the time an individual becomes aware that their data is accessed, it does not necessarily indicate that their data has been repurposed for criminal activity.

There are many government organizations, that provide information to an individual at the time a privacy incident is communicated to the victim, in which their personal identifiable information is exposed. For example, the Office of the Privacy Commissioner, RCMP Anti-Fraud Center, and the Federal Trade Commission provides guidance, and checklists as to the necessary steps required to ensure that the compromised individual remains intact and accessed personal identifiable information (PII) is flagged in critical systems (i.e., government, financial, banking etc.) with Police reports filed in impacted jurisdictions to support prosecution of the criminal.

As a victim of identity fraud resulting from a confirmed privacy breach at Bank of Montreal, and expose PII at PayPal, Equifax, Canada Revenue Agency, Blackbaud, DocuSign, Association of Professional Engineers of Ontario following the process outlined by the Federal Trades Commission, Office of Privacy Commissioner and RCMP Anti-Fraud Center is imperative. Once re-purpose of accessed data is in play, the effects of identity takeover on owns life is daunting. Usually, the ability to takeover one's identity in government, financial, academic, employer and relevant systems require authority, and the fraudster may carry on a life parallel to the victim where their activity goes unnoticed by the victim, as jurisdiction and lifestyle plays a significant factor. At the time the victim realizes that there is a fraudster, it becomes extremely difficult for the victim, as the law in place is to prosecute the criminal, and it neglects the victim.

Countering Identity Takeover Incidents – A Concrete Example

Blog @ https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/countering-identity-takeover-incidents.

The victim (Tara Kissoon, tara_kissoon@it-rs.org) is an active Alumni of the Rotman School of Business at the University of Toronto. This incident occurs in 2020, at the time the fraudster exercising some level of authority applies to represent the University of Toronto, College of Electors, as the active Rotman School of Management Alumni, the victim is unaware.

The University completes the application vetting process of the fraudster (Tara Kisson) with references and allows the fraudster to represent the business school, as the Alumni for a period of two years. The rationale for allowing this fraudster to assume the Rotman Alumni seat is that they are accompanied by a person with authority who verifies that the fraudster as the "real" individual with fraudulent government issued identification that appears to be valid.

The victim, who is the graduate and Alumni is notified by the University's governance committee accidentally during COVID-19 through the distribution of meeting minutes on an unknown email (tarakissoon@it-rs.org) associated with her company-own domain (it-rs.org), which is actively being used by the fraudster and the victim is unaware.

The victim notifies the University that there is a person trying to perform identity takeover, reports this incident to the RCMP Anti-Fraud Centre and attempts to file a Police report which is rejected by the Toronto Police Service in jurisdiction.

The uncovered rationale for this behaviour by the Police is that the fraudster is accompanied by a person of authority who verifies the fraudster as the "real" individual using fraudulent government issued identification. Therefore, the University of Toronto and the Toronto Police Service believes the fraudster to be the "real" individual. The fraudster's motive is to become part of the Rotman Alumni Network with the end goal of an influential lifestyle.

A second example occurs during the period the victim exercised at LA Fitness in Markham, ON Canada. Unknown to the victim, a person impersonating the victim gained entranced to LA Fitness by using the victim's name and fraudulent government issued identification. This continued for several years, even after the victim's membership was cancelled. Evidence is well documented in the York Region Office of the Independent Review Director's Report.

However, no action was taken by the Police. The uncovered rationale for this behaviour by the impersonator is that the fraudster targeted the victim to gain access to the COVID-19 vaccine certificates, personal identifiable information and personal health information, (i.e. health card number).

The fraudster's motive is to integrate within the communities of the victim, to learn the victim's network, behavioural patterns and commit financial crime. Evidence is well documented in the York Region Office of the Independent Review Director's Report and Police Reports file in jurisdiction which include the following: 1) excessive re-issue of the victim's credit card due to fraudulent charges, 2) the re-use of the victim's social insurance number, 3) the re-use of the victim's financial licence, 4) Canada Revenue Agency (CRA) account takeover, 5) monies missing from several accounts, 6) the use of the name **KISSON** on the Equifax and TransUnion credit reports, and 7) targeted attacks on the victim's car and home. However, no action was taken by the Police.

The horrifying truth is that the Police targets the victim and makes the victim's life extremely difficult. The Police refuses to either meet with the victim or perform identify verification. The victim writes: 1) the Office of the Prime Minister, 2) Open Parliament, 3) the Office of the Solicitor General, 4) the Ombudsman's office, and 5) the Ministry of Attorney General. She is instructed to file complaints against the Police for their unlawful activities against the victim, as the civilian Police may be involved.

This bold, public behaviour by the fraudster continues over many years using a derivative of the victim's full name on fraudulent government issued identification, and is present on the victim's credit reports. This comes to the attention of the victim during correspondence with a Police Officer in York Region regarding a different concern. This is reported to the Office of the Independent Review Director (OIPRD) through a complaint against the reporting Police Officer in York Region, as the Police Officer refuses to correct the name in the Law Enforcement system to match the name on the enhanced security Canadian driver's license. This is evident in the report that was provided via text message on July 31, 2023 @ 8:01 AM with a cover page showing the use of the derivative name.

What is most astonishing about this behaviour is the Lead Investigators assigned through the Office of the Independent Review Director (OIPRD) to assess the victim's numerous complaints against the York Regional Police and Toronto Police Service, interviews all of the civilian witnesses except the individual filing the complaint, and it includes Police Officers that have directly interacted with the fraudster, knows the clear identity of the fraudster however, the OIPRD still refuses to either approve the Police report or arrest the fraudster under the criminal code.

Although there is overwhelming evidence provided by the victim through the RCMP Anti-Fraud Center, OIPRD, and numerous police reports filed in jurisdiction, in addition to the victim's identity verification, her Enhanced Police Information Check (E-PIC), Vulnerable Sector Check, Biometrics, NEXUS, Bail Verification, medical/dental records and in-person meeting with the Office of the Independent Review Director (OIPRD) at the York Region Administrative Center on Aug. 23, 2023 @ 10 AM (17250 Yonge Street, Newmarket), an arrest of the fraudster is pending.

This neglect by the Police leaves the victim's life impacted specifically work, marriage, children, income, government taxes, social assistance, OSAP funding, entrepreneurial activities, church and volunteer activities.

Resulting in the victim reflecting on role of the Police in society and the adequacy of the government structure in place to provide strong governance over this type of unlawful activity completed by the Police, and protection of a citizen's personal information against unlawful re-use.

Most of the evidence for this allegation is well documented in three versions of the final report by the lead investigators assigned by the OIPRD in York Region, and the final report issued by the OIPRD in Toronto which demonstrates that the fraudster is well known by the Police in both jurisdictions. It is important to note that both jurisdictions refused to interview the "real" person, who is the individual filing the complaints, instead deleted and rejected all of the 15+ police reports filed in jurisdiction that clearly demonstrate occupational fraud is in play to support financial gain and change in lifestyle.

The Association of Certified Fraud Examiners (ACFE) 2022 *Report to the Nations on Occupational Fraud and Abuse* provides some insight into the people behind the crimes for the 2,110 occupational fraud cases analyzed in this study: [6]

- 23% were owners/executives.
- 58% collaborated with 2+ individuals in committing their scheme.
- 54% were between the ages of 31 and 45.
- 56% had worked for the victim organization for less than six years.
- 65% had at least some university education.
- 49% worked in the accounting, executive, operations, sales functions of the victim organization.
- 87% were first-time offenders with no criminal history of fraudulent behaviour.
- 8% of the cases involved the use of cryptocurrency for kickbacks/bribery payments.

This report shows that recognizing the signs displayed by fraudsters can help organizations more effectively detect fraud and minimize losses. Eighty-five percent of fraudsters display at least one behavioural red flag. These are the eight most common behaviour signs of occupational fraud:

1. 39% were known to be living beyond their means.
2. 25% have financial difficulties.
3. 20% usually have close associations with vendors/customers.
4. 13% have control issues, unwilling to share duties.
5. 12% show signs of irritability, suspiciousness, or defensiveness.
6. 12% shows signs of bullying, intimidation.
7. 11% have divorce/family concerns.
8. 10% have a "wheeler-dealer" attitude

Fifty eight percent of the 2,110 cases analyzed within this study were referred to law enforcement, with 66% of cases resulting in a conviction (808 cases – 38%).

Why Implement Secure Measures to Meet Data Protection Laws?

The above mentioned example of identity takeover is one of the many reasons why cyber terrorism impacts the masses, with one Privacy breach there are potentially millions of victims with exposed personal identifiable information available for re-use. An appropriate governance structure is required to be in place in organizations that have a responsible to be in compliance with privacy and data protection laws, regulations and industry standards.

[6]The Association of Certified Fraud Examiners (ACFE) 2022, Report to the Nations on Occupational Fraud and Abuse, viewed December 7, 2023, http://www.acfe.com/rttn.

The primary reason why funding secure measures in organizations are important is to protect organizations from data and privacy breaches which result in this type of impact to citizens.

Digital Privacy and Data Protection

Digital privacy is the practice of protecting information, which is accessible on the internet, and facilitates mechanisms of using this information in a secure manner, without leaking or compromising the information. Digital privacy is inclusive of protection of an individual's data which is created, accessed, collected and disclosed through electronic means. Throughout the years, use of the internet has transformed the way an individual manages their information, with rapid accessibility by unknown third parties.

Industry reports have shown that there is an increase in the number of reported data breaches where an individual's information is exposed and used in a fraudulent manner.

"The individuals most commonly affected by a Real Risk of Significant Harm (RROSH) breach are customers/clients. They are affected in 56% of reported RROSH breaches. Employees are the second most affected group. The types of harm arising from breach reports largely reflect the evolving causes of breaches and the personal information at issue in these breaches. Identity theft, fraud and risk of financial loss have been constants. More recently, phishing as a harm has been increasing, as more reported breaches involved stolen or compromised email addresses."[7]

Therefore, data protection laws are important to provide a legal framework to manage online privacy. These laws vary across different countries with the enforcement process dependant on the jurisdiction.

Data Protection

One of the most important data protection legislations enacted to date is the General Data Protection Regulation (GDPR). Currently, there are more than one hundred and twenty countries that have enacted legislation to secure the protection of data and privacy.

The European Union's (EU) General Data Protection Regulation, implemented in May 2018, brought data protection into the public and is considered a landmark privacy law with the introduction of new rights for individuals, such as the Right to be Forgotten and the Right to Portability.

The European Union's (EU) General Data Protection Regulation (GDPR) encompasses ten key areas that apply to data protection. Within the scope of this regulation, there are three specific requirements which were taken into account: 1) personal data breaches, 2) privacy by design, and 3) data protection impact assessment.

Within the law, the requirements to evaluate the data security risk with the implementation of appropriate controls are evident. "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.

[7] PIPA Breach Report 2022, viewed September 2023, https://oipc.ab.ca/wp-content/uploads/2022/07/PIPA-Breach-Report-2022.pdf.

Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."[8]
This article shares a strategic framework that could be used by various stakeholders involved in the implementation of cybersecurity measures to safeguard sensitive data and leverages a data centric focus on the evolution of cyber-attacks. Specific security measures are important and should be implemented appropriately to alleviate cybersecurity threats. The information provided in this article will give the necessary data to show that the cybersecurity decision-making process is clearly integrated with risk management methodologies.

Optimal Spending on Cybersecurity Measures

The Book Optimal Spending on Cybersecurity Measures: Risk Management [9] discusses the cybersecurity risk management process which facilitates business driven risk assessments to meet current regulations and industry standards. There are eight case studies which are based on completion of business driven risk assessments in a University setting.
Within the book, Optimum Spending on Cybersecurity Measures: DevOps [10], the Cybersecurity Risk Management Framework is shown through a case study methodology with the elements necessary to create a defensible way of assessing risk, with the implementation of adequate internal controls to ensure the protection of data and privacy as required by law [11].
The Books Optimal Spending on Cybersecurity Measures: Digital Privacy and Data Protection and Optimal Spending on Cybersecurity Measures: Protecting Health Information, highlights the laws in place to protect a citizen's personal information and integrates the cybersecurity risk management framework within the privacy impact assessment (PIA) process to address the potential exposure of personal identifiable information (PII) and personal health information (PHI).

[8] European Union Agency for Networks and Information Security, Octave v2.0, viewed May 2020, https://www.enisa.europa.eu.

[9] Kissoon, T. 2022. Optimal spending on cybersecurity measures: Risk Management (ISBN: 9781032061405). Taylor & Francis: Routledge.

[10] Kissoon, T. 2024. Optimal spending on cybersecurity measures: DevOps (ISBN: 9781032518947). Taylor & Francis: Routledge.

[11] European Union Agency for Networks and Information Security, Octave v2.0, viewed May 2020, https://www.enisa.europa.eu.

Conclusion

Although cyber terrorism is not new, there are continuous emerging attack vectors, and the impact this has on citizens in society is unrealized. The impact identity takeover has on an unsuspecting victim is beyond words and from personal experience it changes one's behaviour. In saying this, awareness should be provided to police officers in jurisdictional precincts on occupational fraud and and use of fraudulent government issued identification, as the victim should not be targeted by police officers. There should be a process in place within the local law enforcement community to assist a victim and ensure identity restoration is achieved.

Organizations recognize the cost of implementing secure measures which include compliance with required regulations, laws and industry standards. Incurring the cost of secure measures is usually aligned to an organization's risk appetite (i.e., risk averse, risk neutral, risk taking). The cost of implementing secure measures does not include the cost of sustaining and recovering from a breach of sensitive data. In conclusion, it is apparent that industry organizations are focused on staying abreast of emerging trends within cyber terrorism to ensure regulations, laws and industry standards are current, enforced and aligned with necessary secure measures to protect citizens.

References

1. European Union Agency for Networks and Information Security, Octave v2.0, viewed May 2020, https://www.enisa.europa.eu.
2. FORGEROCK Identity Breach Report - 2022, 2023, viewed October 2023, https://www.forgerock.com/resources/analyst-report/2023-forgerock-identity-breach-report.
3. KISSOON, T. 2024. Optimal spending on cybersecurity measures: DevOps (ISBN: 9781032518947). Taylor & Francis: Routledge.
4. KISSOON, T. 2024. Optimal spending on cybersecurity measures: Digital Privacy and Data Protection (ISBN: 9781032802473). Taylor & Francis: Routledge.
5. KISSOON, T. 2020. Optimum spending on cybersecurity measures. Emerald Publishing Ltd.: Transforming Government: People, Process and Policy.
6. KISSOON, T. 2021. Optimum spending on cybersecurity measures: Part II. Journal of Information Security.
7. KISSOON, T. 2024. Optimal spending on cybersecurity measures: Protecting Health Information (ISBN: 9781032823577). Taylor & Francis: Routledge.
8. KISSOON, T. 2022. Optimal spending on cybersecurity measures: Risk Management (ISBN: 9781032061405). Taylor & Francis: Routledge.
9. Met Police Officers at Risk After Serious Data Breach, viewed September 2023, https://www.bankinfosecurity.com/met-police-officers-at-risk-after-serious-data-breach-a-22947.
10. PIPA Breach Report 2022, viewed September 2023, https://oipc.ab.ca/wp-content/uploads/2022/07/PIPA-Breach-Report-2022.pdf.
11. Qakbot Malware Disrupted in International Cyber Takedown, viewed September 2023, https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown.
12. The Association of Certified Fraud Examiners (ACFE) 2022, Report to the Nations on Occupational Fraud and Abuse, viewed December 7, 2023, http://www.acfe.com/rttn.
13. United Nations Conference on Trade and Development, viewed on July 13, 2023, https://unctad.org/page/online-consumer-protection-legislation-worldwide.