



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Decoding Cyber & Board Governance

Michael Castro, Presenter
Karen Fryday-Field, Moderator






www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Introductions

www.governforimpact.org




A Bit about Me...

- Last 20+ years in IT,
Primarily Information Security
(also known as Computer
Security, Network Security, IT
security and Cyber.)

Last role as Head of Cyber
Information Security
Management and Risk at Loblaw
Companies.

Today, Principal of RiskAware, a
boutique Cybersecurity company
promoting Advisory services for
Boards, Sr. Leaders and SMB as
well as vCISO and traditional
cybersecurity services



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Goals for the session

www.governforimpact.org

GOVERN
for **IMPACT**
Empowered Boards.
Re-imagine the world.

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

An Overview of the Nature of CyberSecurity



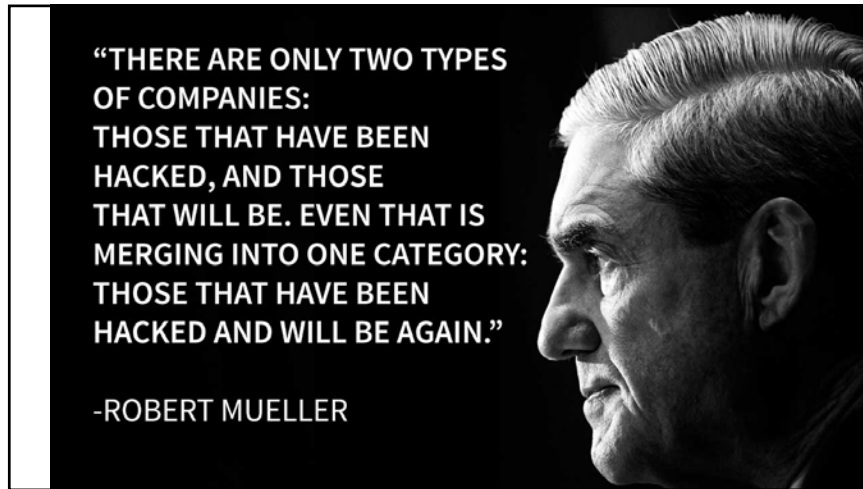
www.governforimpact.org



**IF THERE'S ONE THING
THAT'S CERTAIN IN BUSINESS
IT'S UNCERTAINTY**

Stephen Covey, Author

Cyber risks are upon us as
businesses **grow** and
transform



GOVERN for IMPACT
Empowered Boards. Re-imagine the world.

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

General Trends in Business

- INDUSTRY 4.0
- SUPPLY CHAIN AUTOMATION AND TRANSPARENCY
- LOYALTY THROUGH CONVENIENCE
- DIGITAL PAYMENTS
- ECOMMERCE EVERYWHERE
- DATA DRIVEN INSIGHTS AND ANALYTICS
- COGNITIVE TECHNOLOGIES (AI, ML, RPA)
- M&A

www.governforimpact.org



GOVERN for IMPACT
Empowered Boards. Re-imagine the world.

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

10B devices already on the Internet (2017)

Expected to **DOUBLE** by 2020 **75B** by 2025

Projected traffic to be **44 zettabyte** or **44 trillion GB** in next 5 years

In the future **99%** of everything we make will connect to the Internet.

www.governforimpact.org

Automation in Supply Chain

Shoppers Drug Mart location using robotic dispenser

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

SYDNEY - A Sydney pharmacy has introduced a new robotic dispensing system, but it hasn't resulted in a loss of work for any of its staff.

The Shoppers Drug Mart located at the Sydney Shopping

FINANCIAL TIMES

Amazon robots bring a brave new world to the warehouse

Shelf-carrying machines wait along effortlessly in a new logistical dance

HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

PHOTO/VIDEO OP - Hudson's Bay Company Unveils First-in-Canada Robotic Fulfillment Technology at Scarborough Distribution Center; Most Advanced Technology in the Industry

www.governforimpact.org

COUNCIL on FOREIGN RELATIONS

Trending Iran Deal Korean Peninsula Afghanistan Immigration Trade

Member Login

from Net Politics and Digital and Cyberspace Policy Program

The Quantum Race the United States Can't Afford To Lose

The quantum race is on, and the stakes are high. The winner will gain a military and intelligence edge, as well as a first mover advantage in what is guaranteed to be a massive industry for decades to come. How will the United States fare?

Blog Post by Guest Blogger for Adam Segal
April 18, 2018

A 2-Way Quantum processor is pictured during a media tour of the Quantum Artificial Intelligence Laboratory (Q-AI2) at SLAC Area Research Center in Menlo Park, California on December 4, 2017. Stephen Lee/Reuters

www.governforimpact.org

How quantum computing could wreak havoc on cryptocurrency

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

by RAZ RAFAELI — 1 day ago in CONTRIBUTORS

Quantum Hacking Could Be 'Catastrophic' If We Don't Develop Better Cryptography

Ryan F. Mandelbaum
2/16/18 5:00pm • Filed in: QUANTUM COMPUTERS

Your data may be safe from a quantum attack... for now. When quantum computers develop the ability to crack present-day encryption mechanisms, will you be ready?

CSO

Cryptomining: the new lottery for cybercriminals

With more than 500 million PCs actively mining cryptocurrency worldwide, you have to wonder how many compromised websites exist.

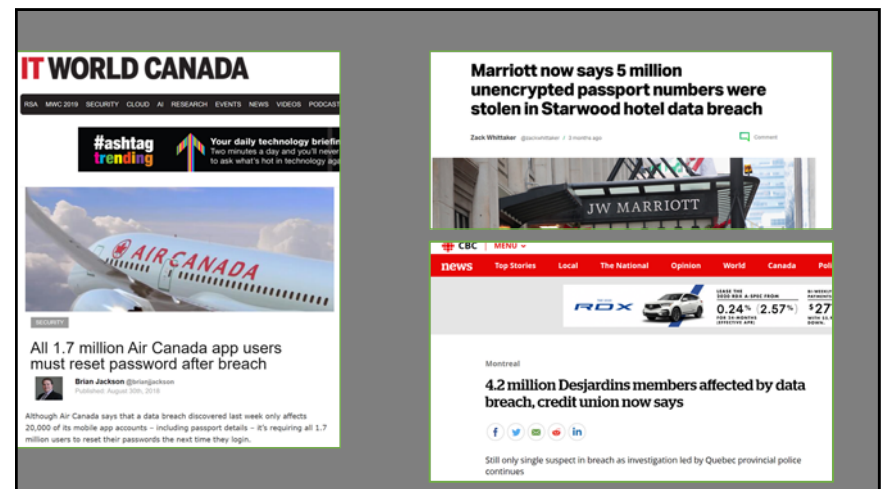
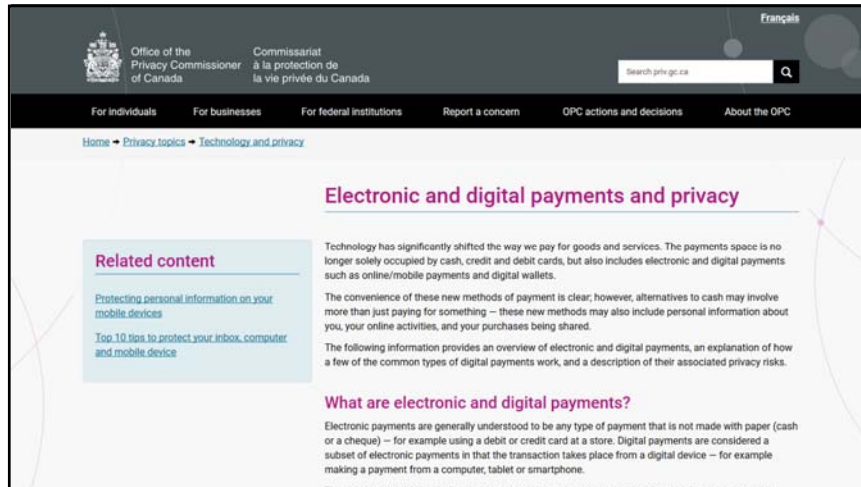
Roadmap
New York City • July 12, 2018
REGISTER

MORE LIKE THIS

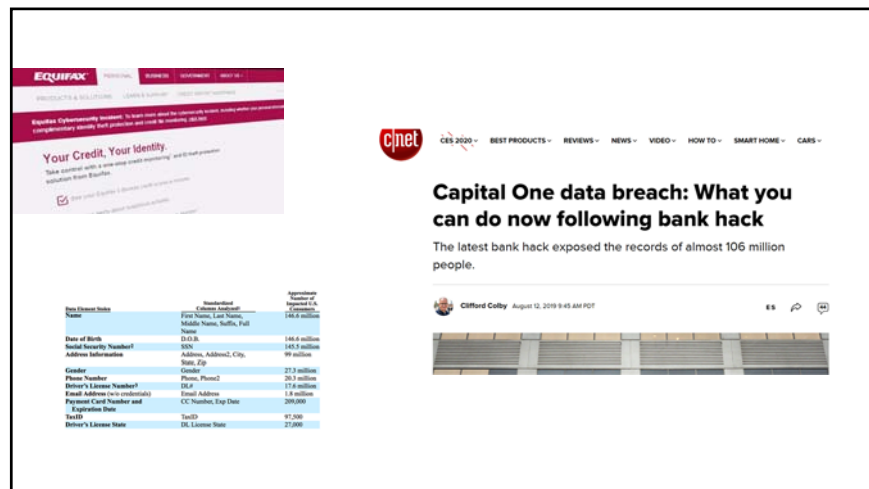
What is cryptopacking? How to prevent, detect, and recover from it

Banned Hackers want you...

The materials provided by the faculty for this GOVERN for IMPACT advanced practice webinar are of a proprietary nature. Any replication of the materials or providing them to a third party without the explicit consent of the faculty member of GOVERN for IMPACT is prohibited.



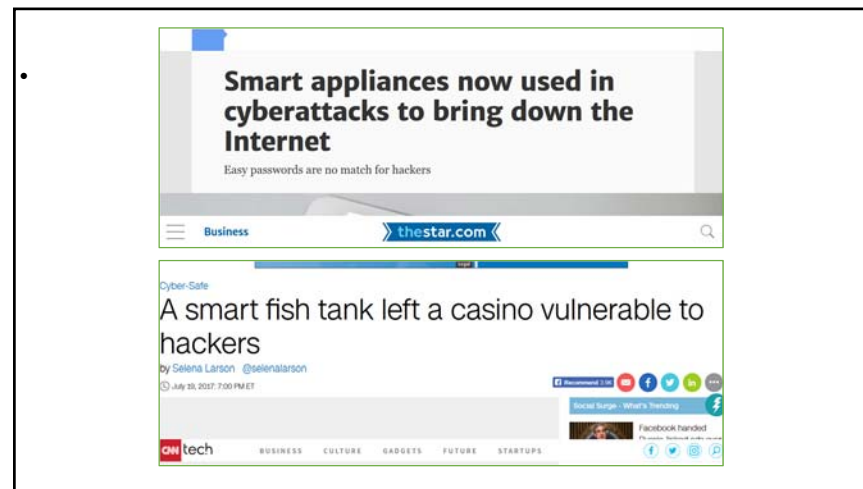
The materials provided by the faculty for this GOVERN for IMPACT advanced practice webinar are of a proprietary nature. Any replication of the materials or providing them to a third party without the explicit consent of the faculty member of GOVERN for IMPACT is prohibited.



Capital One data breach: What you can do now following bank hack

The latest bank hack exposed the records of almost 106 million people.

Data Breach Title	Number of Records	Estimated Monetary Loss
First Name, Last Name, Middle Name, Suffix, Full Name	146.4 million	\$14.4 million
Date of Birth	146.4 million	\$14.4 million
Social Security Number	146.4 million	\$14.4 million
Address Information	99 million	\$9.9 million
Gender	27.2 million	\$2.7 million
Phone Number	26.1 million	\$2.6 million
Driver's License Number	17.4 million	\$1.7 million
Email Address (no email domain)	1.4 million	\$0.1 million
Payment Card Number and Expiration Date	209,000	\$20.9 million
Twitter	97,200	\$9.7 million
Driver's License State	27,000	\$2.7 million



Smart appliances now used in cyberattacks to bring down the Internet

Easy passwords are no match for hackers

A smart fish tank left a casino vulnerable to hackers

by Selena Larson @selenalarton
July 28, 2017 7:00 PM ET



LifeLabs
@LifeLabs

We recently identified a cyber-attack that involved unauthorized access to our computer systems. We are sorry that this incident happened. The data has been retrieved, and a law enforcement investigation is underway. For more info, visit customernotice.lifelabs.com.

53 1:27 PM - Dec 17, 2019

273 people are talking about this

LIFE LABS DATA BREACH: 15 MILLION PATIENTS AND THEY PAID RANSOM TO GET THE DATA BACK!

ONTARIO SECONDARY SCHOOL TEACHERS FEDERATION L.L. 6:36 AM



Travellex

Latest press release:
"Press release just issued"
07 January 2020.

Updated Travellex Statement on Cyber Incident

On Tuesday December 31st Travellex detected a software virus which had compromised some of its services. As previously announced, on discovering the virus, and as a precautionary measure, Travellex immediately took all its systems offline to prevent the spread of the virus further across the network.

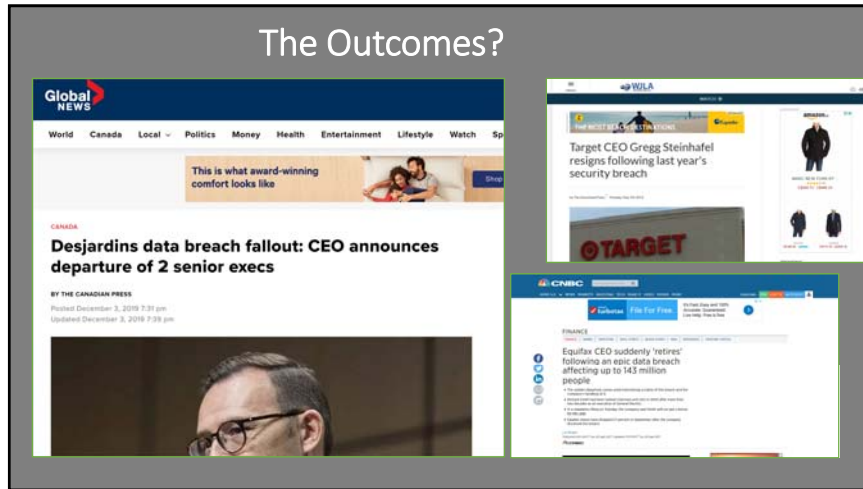
Whilst the investigation is still ongoing, Travellex has confirmed that the software virus is ransomware known as Sodinokibi, also commonly referred to as REvil. Travellex has proactively taken steps to contain the spread of the ransomware, which has been successful. To date, the company can confirm that whilst there has been some data encryption, there is no evidence that structured personal customer data has been encrypted. Whilst Travellex does not yet have a complete picture of all the data that has been encrypted, there is still no evidence to date that any data has been exfiltrated.

Having completed the containment stage of its remediation process, detailed forensic analysis is fully underway and the company is now also working towards recovery of all systems. To date Travellex has been able to restore a number of internal systems, which are operating normally. The company is working to resume normal operations as quickly as possible and does not currently anticipate any material financial impact for the Finablr Group.

Tony D'Souza, Chief Executive of Travellex, said "Our focus is on communicating directly with our partners and customers to protect them and their information from any further compromise. We take very seriously our responsibility to protect the privacy and security of our partner and customer's data as well as provide an excellent service to our customers and we sincerely apologise for the inconvenience caused. Travellex continues to offer services to its customers on a manual basis and is continuing to provide alternative customer solutions in the interim. We are working tirelessly to bring our systems back online."

Travellex is in discussions with the National Crime Agency (NCA) and the Metropolitan Police who are conducting their own criminal investigations, as well as its regulators across the world.

The materials provided by the faculty for this GOVERN for IMPACT advanced practice webinar are of a proprietary nature. Any replication of the materials or providing them to a third party without the explicit consent of the faculty member of GOVERN for IMPACT is prohibited.



GOVERN for IMPACT
Empowered Boards. Re-Imagine the world.

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

As Leaders you need to be aware



FINANCIAL



REPUTATION



SHARE VALUE

www.governforimpact.org

GOVERN for IMPACT
Empowered Boards. Re-Imagine the world.

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Domino Effect on Security Incidents

The diagram shows a series of dominoes falling in a sequence. The dominoes are labeled with the following text from left to right: "Negative social media coverage", "Employees unable to access systems", "Extreme pressure on operations", "Forensic investigations", "Negative local/national press", "Cost of alerting customers", "Contractual breach", "Regulatory investigations", "Reputation costs", "Loss of customers", "Loss of sales", "Loss of jobs", and "Loss of organization/ business".

Domino effect on security incidents

www.governforimpact.org






Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Description of Labelling the Different Types of Cyber Risk

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Here is a list of the kinds of cyber attacks mostly faced by business:

- **Advanced Persistent Threats (APT):** It is where a hacker gains access to a system or network over a long period of time with the intention to gather data or for a more extensive attack later on.
- **Phishing:** Hackers target mainly emails or another online form of communication to perform vulnerabilities.
- **Denial of Service (DoS):** It is the attack in which the hacker usually sends excess messages requesting the server to authenticate requests leading to an invalid return address. It may shut down your system making it inaccessible to the actual users.
- **Malware:** This virus gets downloaded in the system without the user's knowledge to have access to sensitive data and information from the system.
- **Ransomware:** In this attack, the hacker gathers data from the system and also prevents the user access unless a "ransom" fees are paid.
- **Man in the Middle (MITM):** this is where the 3rd party gains access to the communication and then gains access to monitor any information shared over the connection.

www.governforimpact.org

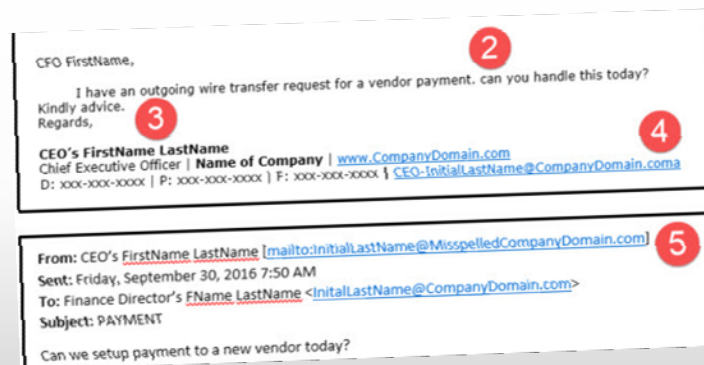
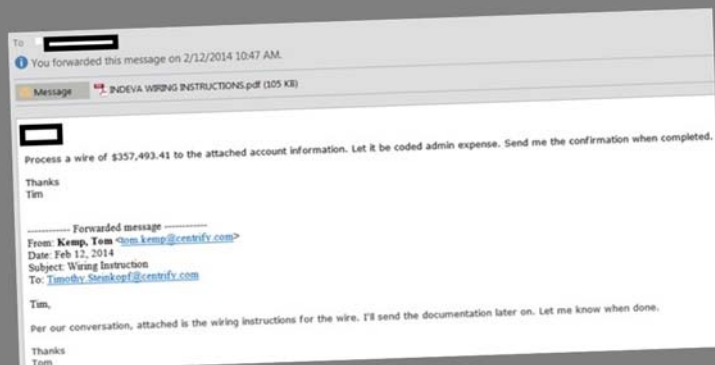


The materials provided by the faculty for this GOVERN for IMPACT advanced practice webinar are of a proprietary nature. Any replication of the materials or providing them to a third party without the explicit consent of the faculty member of GOVERN for IMPACT is prohibited.



CEO Email Fraud: Vulnerable Employees, Lucrative Gains

- Who within your company holds the most power and authority? Chances are, it's your CEO, and attackers are taking advantage of this by impersonating their email addresses in order to acquire money and information for financial gain





Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Decoding the Needs of Leaders Today

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Five wooden blocks arranged to spell out the word 'TRUST'. Each block has a small number '1' in the bottom right corner.

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Cyber is creeping up on Top Risks Boards need to face

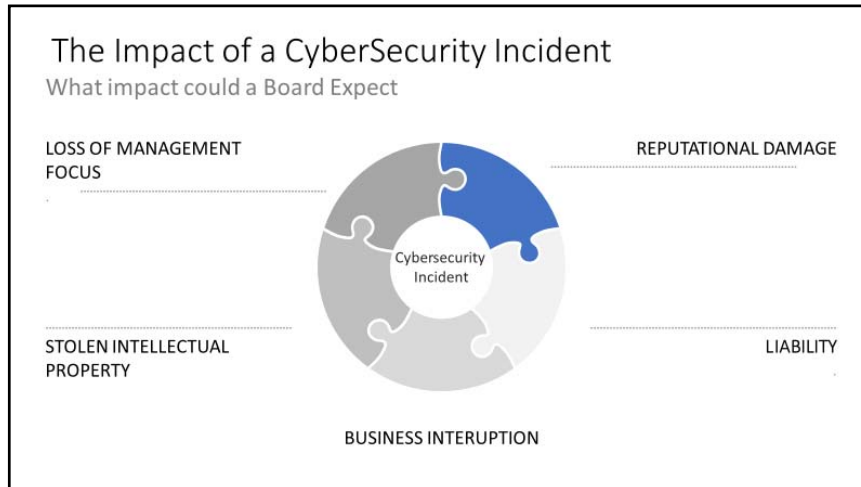
www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

The Impact of a CyberSecurity Incident

www.governforimpact.org



GOVERN
for **IMPACT**
Empowered Boards.
Re-imagine the world...

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Innovative IT transformation initiatives keep expanding the digital footprint, and are outpacing the security protections companies have in place

www.governforimpact.org

GOVERN
for **IMPACT**
Empowered Boards.
Re-imagine the world...

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Key Considerations for the Board

www.governforimpact.org

Know what The “Crown Jewels” are and What efforts are being taken to Protect them

Every organization has its Crown Jewels

Knowing what they are, where they are, and the criticality and impact if they were to be lost is paramount

Boards need to know this before they are lost or compromised

Cyber Threats are Everchanging and Morphing



With changing threats comes need for changing methods of protection



Boards need to be Aware on What the company is doing to detect and respond to these new threats



Boards need to ensure assessments of risk is continually performed

Your organization is Growing and with it must Cybersecurity



Innovation and Digital growth are evolving how companies do business



Cyber is about risk but is also about staying resilient and keeping up with Transformation

Your Company has already been Impacted by Cyber whether Large or Small



It is not about If or even When anymore.. It has already occurred



Boards must know how companies are handling their current threats and breaches



Duration and Impact are Vital to Understand



Organizations need to be Prepared



Boards should understand the Incident Response Plan, what it entails and what the roles are



Board members have a piece to play

Not knowing is no Longer an Argument



Boards need to know what is being done (and not being done) for Cyber within the organization



Regular updates from the IT teams and Security Teams help Board members have a glass into the efforts




Updates need to include Roadmaps, Metrics, Incident Updates and articulation of Risk



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Cyber Governance for the Board

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

The National Association of Corporate Directors (NACD), *Director's Handbook on Cyber-Risk Oversight* outlines five core principles that all board members of public companies, private companies, and non-profit organizations of all sizes and in every industry sector should consider "as they seek to enhance their oversight of cyber risks."

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue

As is often the case, organizations look at cybersecurity as an IT issue or a technology issue. The reality is for almost all organizations is that cybersecurity is an enterprise-wide issue and as such needs to be dealt with utilizing an enterprise-wide risk management process.

Most reporting will continue to come from IT or where cybersecurity typically rests in the organization (usually IT but could be legal or privacy). Impacts are organization-wide and handling it reversely is the best approach in dealing with stemming cyber issues.

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Directors should understand the legal and regulatory implications of cyber risks as they relate to their company's specific circumstances

Directors are coming under the microscope more than ever for cybersecurity. The duty of care for board members is to see security as a key part of their risk reviews, sometimes in the top three. With the responsibility of their roles comes accountability as well.

Executive management along with board members, are being held accountable for many high profile breaches, and in many cases losing their positions.

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the Board meeting agenda

For boards to understand cybersecurity, they need to be knowledgeable as a board member or have access to someone who is. Many boards have looked to strategic advisors who can provide board members with advice and insight into the topic and how it has a bearing on their roles and decisions. However, it is now becoming more common to see board members who either have a technology or security background directly. This expertise allows the board as a whole to be more elevated in awareness and with it, become better prepared.

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget

It is important for board members to have a discussion on understanding the risk associated with cybersecurity. Like many risk items, understanding where cyber sits in the discussion will help prioritize the funding, priority and responsibility as boards navigate the sometimes treacherous cybersecurity landscape.

Of course, risk is always a fine balance. An organization cannot be totally risk-averse. This can lead to lack of innovation and new opportunities. As such, organizations have to find that balance between risk and opportunity.

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach

It is imperative that Boards set the tone for cybersecurity for an organization. A large portion of this is to expect that an enterprise-wide framework for risk management is used


www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Cyber Conversations for the Board

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Typically the questions have been very and broad, often due to the lack of cyber knowledge available on the board. Questions would often be along the lines of:

- Are we secure?
- How will we know if we have had a breach?
- How does our security program compare with industry peers and competitors?
- Do we have enough resources for our cybersecurity team?
- How effective is our security program?

In reality, board members need to be concise and directly engaged and ask questions that draw the conversation to tangible actions by senior leadership and the CISO. All of the board members need to draw definitive results that can help

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

More appropriate questions should be similar to:


What evidence does the Board have that the CEO has ensured cybersecurity has and is being addressed (e.g. a written data privacy and cybersecurity program consisting of suitable policies and procedures)?

It is imperative that the CEO ensures written policies for data privacy and cybersecurity that are reviewed regularly.

What evidence is there that the CEO has ensured staff are knowledgeable (e.g. security training programs that guide staff on the appropriate handling and protection of corporate data)?

The board should be confident that appropriate staff knowledge and skill is in place for how to deal with security and privacy issues. Questions should be asked to ascertain the compliance to security policies.

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Has senior leadership determined how much of the budget and how many staff are required for providing cybersecurity for the organization?

It is important to have adequate funding for cybersecurity. However it is based on the many factors, including the company and its industry. Funding should be questioned and reviewed as to how it is allocated.

Has senior leadership given thought to purchasing cyber liability insurance?

Senior leadership should be asked if they have considered a liability policy for cyber attacks. If already procured, the questions should center around the scope of coverage and the adequacy for the organization.

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Has senior leadership reviewed the cybersecurity risks associated with partnering with third parties?

Third parties are often seen as the most common threat vector for attacks. As such it is imperative for the organization to review security with their third parties and vendors and ask if those reviews meet the standards of the organization.

Does senior leadership have a written incident response plan?

It is vital for a written plan to be in place that ensures the organization as a whole is ready for any incident. The plan should involve individuals for all teams, be tested regularly with scenarios or tabletop exercises and the plan should be reviewed regularly to ensure it remains up to date.

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

As organizations transition to a digital era, security is becoming the new paradigm. The shift means a movement in the management and appreciation for cyber threats. Business and strategic priorities need to evolve. Boards are now being held accountable and risk their success and own liabilities if not well versed and not prepared. No longer can board members sit and plead ignorance or lack of understanding. They must be engaged. It is imperative to ask the right questions and understand the risk and impacts of cybersecurity to their own organization

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

“ In a networked world,
TRUST is the most
important currency “

Eric Schmidt
Executive Chairman of Google

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Cybersecurity Executive Limitation
Policy – An Example and
Discussion

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Cyber Event at
Target Corp
A Case Study



www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Executive Summary

- In November 2013, Target Corporation was the subject of one of the largest cyberattacks in history.
- Heading into Christmas, the retail industry's busiest season of the year, hackers stole credit and debit card information for 40 million Target customers and names, as well as home addresses and Email for another 70 million.
- The attack and Target's response exposed the company to intense scrutiny and raised questions about the accountability of Target's board of directors and the Audit Committee and Corporate Responsibility Committee that were responsible for the oversight of both operational and reputational risks.
- Leading proxy advisory firm Institutional Shareholder Services (ISS) recommended that Target shareholders vote against the re-election of 7 of Target's 10 board members, including the chair of the Audit Committee.
- Investors filed derivative suits charging the board with breach of fiduciary duty and waste of corporate assets, with lack of diligence in protecting sensitive customer information, and with failure to oversee risks to brand value.
- While Target's board vigorously defended its performance, observers were left wondering about the extent of board accountability for a breach of such large magnitude.

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Company Background

- Company roots date back to 1902
- Target first emerged in 1962, same time as Walmart and Kmart
- In 2013, Target operated 1,919 stores including Canada
- Revenues of over **\$72 Billion**
- Thanksgiving to Christmas represented busiest Quarter
- For 2013 Christmas, staff increased by 50 000 to 415 000
- 30% of annual revenue derived in this period

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

The Start of the Cyber Troubles

- September 2013 – Target gains **payment card industry (PCI)** certification, a cybersecurity requirement for organizations that accept credit cards. Certification attests to specific controls for cyber
- September 2013 - Hackers from an unknown location initiated a phishing Email campaign against one of Target's external heating and ventilation providers, **Fazio Mechanical Services**. At the time, Information about Target's vendors was publicly available online and hence accessible to anyone searching it. When a Fazio employee clicked the malicious email, it enabled hackers to steal all of Fazio's passwords.
- Fazio's main method to detect malware was a free version of a security product called "Malwarebytes Anti-Malware" whose license explicitly prohibited corporate use. But Fazio had relied on it anyway, and Target did not monitor this vendor's or most other's security arrangements. (The software was incapable for the threat)
- Around the same time Target's own security team identified vulnerabilities in Target's payment card systems and cash registers, but no further investigations were undertaken or ordered by the company.

www.governforimpact.org

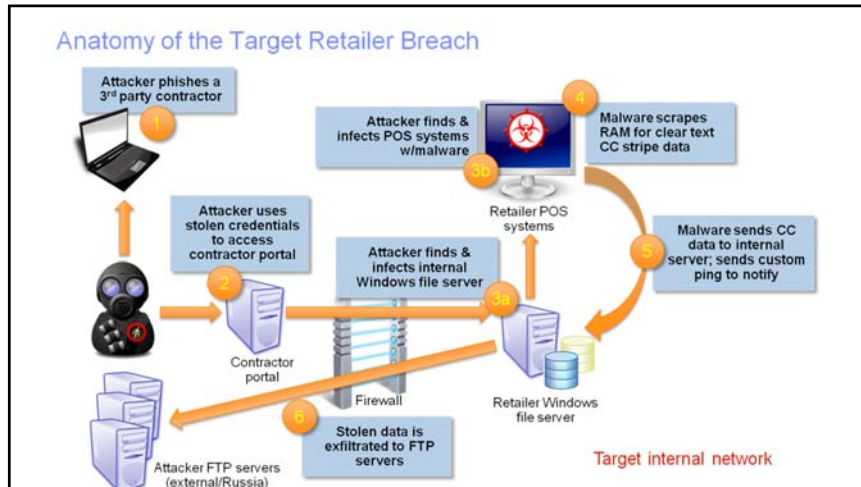


Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

The Gaps

- November 15, 2013 -Using credentials from Vendor, hackers gained access to Target's network for electronic billing, project management, and contract submission (System typical for vendor to access in 3rd party)
- To prevent such an intrusion, Target could have required two-factor authentication—a regular password, enhanced with a verification code sent to the vendor's mobile phone—which was a **PCI standard** for remote access by 3rd parties, but was not being required by Target. (Target only required for its most sensitive connections by select vendors)
- From a technical perspective, Target's network was not properly segmented, and as such, the hackers gained access to sensitive customer payments and personal data.
- For security reasons there should never be a route between a network for an outside contractor (such as Fazio) and the network for payment data. In Target's case, it existed and the hackers found it and exploited it

www.governforimpact.org



The Attacks

- November 15 - Attackers started with infecting a small number of Point of Sale Systems (POS)
- End of November – Majority of systems are infected with Malware, and begin scraping information with each credit card swiped on POS system
- December 2 - Hackers start exporting stolen data from Target systems to an external server in Russia
- In total 11 Gigabytes (GB) of data was stolen representing 40 Million debit and credit card accounts



The Mistakes

- Prior to attacks, Target had contracted cybersecurity company FireEye Inc., a firm that provided malware detection tools and monitoring. These security specialists were required to monitor Target's systems 24/7.
- The FireEye team initially raised an alert of an attack right after the Black Friday shopping season, on November 30th, and the FireEye team sent an electronic alert to Target's in-house security team in Minnesota indicating that the monitoring software had detected malware intrusions but that the install had not been activated yet. However, **the U.S. team did not respond to the alert.**
- Once the malware started extracting the data to the hackers on December 2, the FireEye security team again alerted Target's security team in Minneapolis, **but got no response**
- As well, the software had the ability to delete impacting malware automatically, however this feature had been disabled by the Target Security teams



Target becomes aware

- December 12 - The U.S. Department of Justice (DOJ) contacted Target about the breach, making the company's U.S. executive team aware of its seriousness.
- December 14 - Target hired a 3rd party forensics team to investigate the breach
- December 15 – CEO became aware of breach
- December 15 - Target began removing the malware from its systems and the attackers started losing access to the Target network, but Target wanted to avoid disruption in store operations and **did not close its stores**
- December 18 – Media releases story of Target breach
- December 19 – One week after being notified, Target posted on its corporate website and distributed through regular media outlets a press release stating that it was "aware of" unauthorized access to payment card data and was taking action



Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

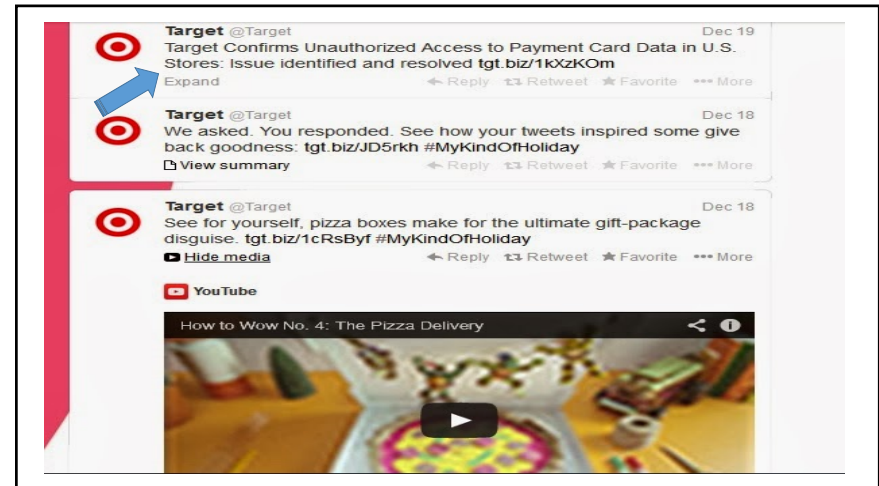
Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.

"Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."

Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

More information is available at Target's corporate website. Guests who suspect unauthorized activity should contact Target at: 866-852-8680.

Source: "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," Target Corporation website, <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-card> accessed July 7, 2016.



Target begins notifying

- Callers to call centre cannot get through or end up with recorded message
- December 20 - CEO Steinhafel explained in a letter posted on Target's website and sent to customers via email and U.S. mail that "there is no indication that PIN numbers have been compromised". The CEO also explained that simply having shopped at Target during this period did not imply that they would be victims of the fraud, and that the level of fraud had been low in similar situations
- December 25-27 - A payment executive familiar with Target's breach stated that PIN information had been stolen, and on December 27, Target **reversed** its earlier position to confirm that PIN information had, in fact, been stolen. In addition to PIN data, CVV numbers and expiration dates had also been compromised, and customers need not have even needed to swipe their cards in a Target store during the period. Target had retained data over time, which had now been stolen

Target's CEO Informs Customers of Data Breach, Dated December 20, 2013

Dear Target Guest,

As you have likely heard by now, Target experienced unauthorized access to payment card data from U.S. Target stores. We take this crime seriously. It was a crime against Target, our team members and most importantly you—our valued guest.

We understand that a situation like this creates stress and anxiety about the safety of your payment card data at Target. Our brand has been built on a 50-year foundation of trust with our guests, and we want to assure you that the cause of this issue has been addressed and you can shop with confidence at Target.

We want you to know a few important things:

The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected.

Even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud.

There is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards. Someone cannot visit an ATM with a fraudulent debit card and withdraw cash.

You will not be responsible for fraudulent charges—either your bank or Target have that responsibility.

We're working as fast as we can to get you the information you need. Our guests are always the first priority.

For extra assurance, we will offer free credit monitoring services for everyone impacted. We'll be in touch with you soon on how and where to access the service.

Please read the full notice below. And over the coming days and weeks we will be relying on target.com, abulleyview.com, corporate.target.com and our various social channels to answer questions and keep you up to date.

Thank you for your patience, understanding and loyalty to Target!



Gregg Steinhafel Chairman, President and CEO, Target
Source: Target Corporation, "A message from CEO Gregg Steinhafel about Target's payment card issues," Target Corporation website, <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-card> accessed May 4, 2016

Target begins notifying

- January 10, 2014 - Target announced that, in addition to payment card data, personal information **including names and mailing and email addresses** had also been stolen for 70 million customers, 30 million more than Target had initially reported

The aftermath to Target

- Target's total sales fell 6.6% for the fourth quarter of 2013, and compared to the previous year, net earnings for the fourth quarter dropped by 46% to \$520 million. As of February 1, 2014, six weeks after the date of the breach announcement, the firm's stock price fell 8.8% to \$56.7 per share. Target also forecasted roughly 20% lower earnings per share (EPS) guidance after the episode.
- Although Target made a concerted effort to control the damage from the attack, it faced extensive media scrutiny, investigations by Congress, the Securities and Exchange Commission (SEC), the Department of Justice, and the Federal Trade Commission (FTC), as well as litigation from affected customers, banks, and shareholders.
- Target faced lawsuits from individual customers, banks that provided credit card services, and investors. On May 7, 2014, Target had 81 consumer cases, 28 bank cases, and 4 shareholder cases filed and pending before various courts
- By 2015, Target had spent roughly **\$290 million** in costs related to the breach and expected a reimbursement of \$90 million from insurers

Board Accountability

- Shareholders of Target filed derivative lawsuits against all directors on the firm's board of directors and against the CFO and CIO. In particular, shareholders identified CEO Gregg W. Steinhafel, CIO Beth M. Jacob, Lead Independent Director James A. Johnson, and chairs and members of the board's Audit and Corporate Responsibility committees as leaders whose "reckless disregard for their duties . . . posed a risk of serious injury to the Company"
- The lawsuits claimed that by their fiduciary duties, the directors were required to create and maintain a system to protect customers' personal and financial information, as well as to inquire into and correct unsound practices. In addition, the directors were required to inform customers of a breach in an accurate and timely manner.
- The derivative lawsuits stated that the directors breached their fiduciary duty by failing to implement internal controls to protect consumer data. In addition, shareholders alleged the directors' negligence caused a waste of corporate assets, as the firm lost revenue, had to offer a 10% discount to draw customers back to the store, and faced upcoming litigation expenses
- Plaintiffs further alleged that the directors and Audit Committee members did not take their financial reporting responsibilities seriously and that they failed to supervise internal controls and cybersecurity systems. Shareholders listed a number of costs incurred by them which eroded shareholder value

Risk Acknowledgement by Board

- The Target board's Audit Committee charter highlighted the committee's oversight responsibility for reviewing and discussing the approach to risk assessment, including the risk of fraud, with the firm's head of internal audit. This collaborative responsibility also included dedicating resources to mitigate identified risks. Target's proxy statement also highlighted the Corporate Responsibility Committee's responsibility for "assessing and managing reputational risk." In a filing, Target had identified data security breach as a risk the firm was exposed to:
- *If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.*

Governance actions against the Board

- Leading proxy advisory firm ISS issued a report in May 2014, stating that “failures of the Audit Committee, the Corporate Responsibility Committee, and the board allowed significant losses to the company and its shareholders”. ISS expressed concern at the “failure of these committees and possibly by extension the full board, to recognize the potential threat faced by the company.”
- ISS advised shareholders that 7 of 10 board members should be removed for their negligence. ISS recommended removal of the entire Audit Committee, including the chair, Roxanne Austin; the Lead Independent Director, James Johnson, who was also on the Compensation Committee; and two other directors

Target Board Fights Back

- After ISS released its report, Target’s board issued a response telling shareholders that it took its “oversight responsibilities seriously” and before the breach had authorized the company to spend “hundreds of millions of dollars” on network security, doubled the information security staff over five years, and taken other security measures. Target also explained that the firm had “300 employees dedicated to information security, trained 350,000 employees on data security, and staffed a 24-hour security operations center to review suspicious network activity.”
- Others defended the board. “The role of directors is one of oversight, not of day to day management. Directors cannot be expected to manage security personnel to ensure that they are doing their job; this role is clearly and squarely a management function. . .”
- Target did identify cybersecurity as a risk, and placed controls to monitor this risk; the oversight was the result of human error.

Target's Interim Chairwoman Roxanne Austin Defends the Board of Directors

To Our Shareholders,
As you make your voting decisions for our 2014 Annual Meeting, we wanted you to have the facts about your Board's oversight of information security practices at Target.

Cyber-crime is a real and persistent threat as sophisticated criminals are constantly seeking to breach information networks and steal data. Breaches are occurring across the economy and are affecting a wide range of victims including the US Government, the technology and defense industries, and more traditional companies, like retailers.

Your Board fully recognizes the importance of its oversight responsibilities in this area. Under the Board's leadership and oversight, Target took significant action to address evolving cyber-crime risks before the breach, by:

- Investing hundreds of millions of dollars in network security personnel, processes, technology and related resources
- Dedicating more than 300 employees to information security (more than double from five years ago)
- Requiring annual data security training for all Target employees (more than 350,000)
- Operating a Security Operations Center (SOC) staffed around the clock with trained professionals to review suspicious network activity
- Investing in network monitoring technology to enhance Target's ability to detect potential cyber-attacks
- Becoming a founding member of the National Cyber-Forensics & Training Alliance (NCFITA), a partnership of public, private and academic participants focused on identifying, mitigating and neutralizing cyber-threats

Despite these efforts, Target suffered a sophisticated criminal attack that led to our data breach in 2013. Since then, your Board has actively monitored Target's response to the situation. Following the breach, the Board has overseen substantial efforts to protect Target's guests. Target is undertaking an end-to-end review of its network security and is moving toward chip and PIN technology for credit card processing. The Board is conducting a broad examination of Target's risk oversight structure, which will include an examination of the role of senior management, reporting structures and Board oversight.

Target has already done the following:

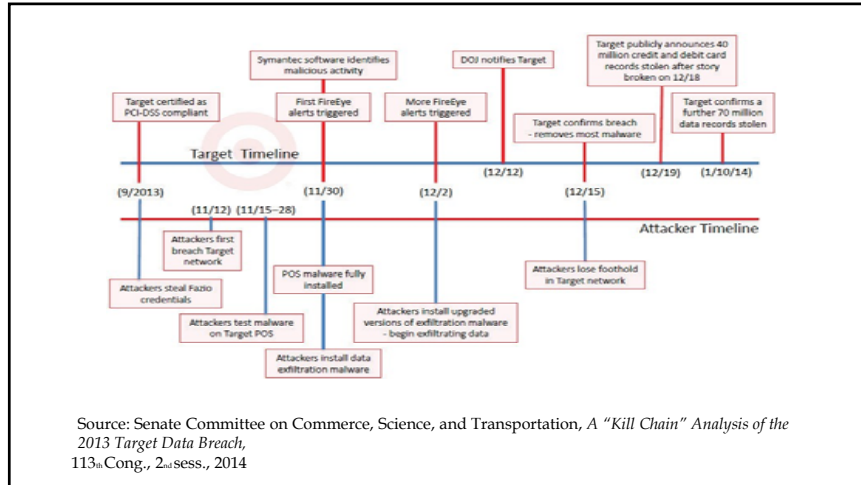
- Announced that we are accelerating the adoption of “chip and PIN” smart payment card technology and set important goals for 2015, including:
- Converting all of our REDcards to chip-enabled cards
- Equipping our stores with chip-enabled card readers
- Hired a new Chief Information Officer
- Elevated the Chief Information Security Officer and Chief Compliance Officer roles and commenced searches to fill those positions


- Enhanced information security decision making processes
- Worked with other leading retailers to establish the Retail Information Sharing and Analysis Center (Retail-ISAC) and joined the Financial Services Information Sharing and Analysis Center (FSISAC) as the first retail member of the group

Again, we want to assure you that the Board takes its oversight responsibilities seriously and we recognize the importance of Target addressing these information security issues in the most effective manner possible. We would appreciate your feedback on this important topic. If you would like to share your thoughts and comments, please send a message to BoardOfDirectors@target.com. We also value your support and ask that you vote in favor of the re-election of all your Target directors at our 2014 Annual Meeting.



Roxanne Austin, Interim Chair of the Board of Directors
Source: Target Def 14A filed June 2, 2014, accessed May 12, 2016.






Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Case Study Questions

- Does it appear that cybersecurity was proactively mitigated at Target? What were some obvious stumbling blocks
- What do you think the culture was for Security at the organization
- Was there a way to prevent this?
- Do you think senior management had a pulse on the risk of cyber to the organization or what was occurring regularly
- What should senior management do now?
- Do you think the Board was proactive prior to this event in cybersecurity?
- What will the Board at Target need to do now?
- Is there a new governance view that needs to be taken by the Board?

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Observations, Thoughts, Takeaways

www.governforimpact.org




Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020



Questions?

www.governforimpact.org


The materials provided by the faculty for this GOVERN for IMPACT advanced practice webinar are of a proprietary nature. Any replication of the materials or providing them to a third party without the explicit consent of the faculty member of GOVERN for IMPACT is prohibited.

GOVERN for IMPACT
Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Michael Castro
@canadaciso
linkedin.com/in/michaelrcastro
mcastro@riskaware.ca

RiskAware



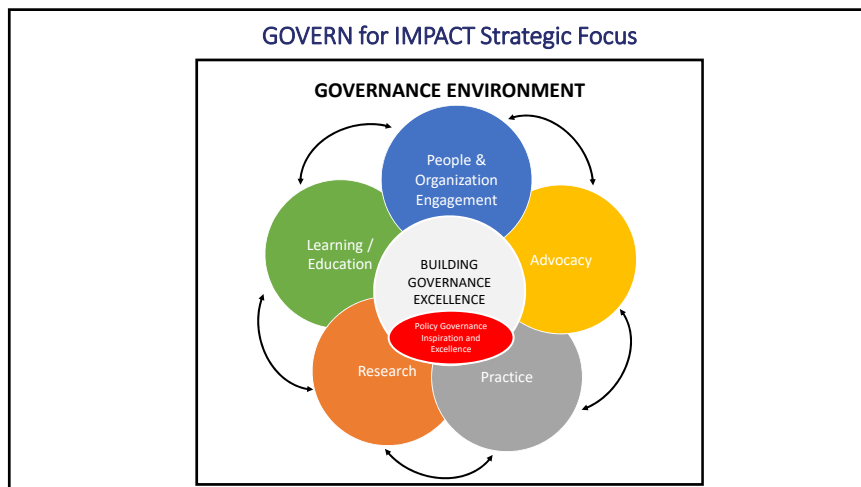
www.governforimpact.org

GOVERN for IMPACT
Empowered Boards.
Re-imagine the world...
Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

KEY AREAS OF FOCUS




www.governforimpact.org



GOVERN for IMPACT
Empowered Boards.
Re-imagine the world...
Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Building Premium Products + Services

- Best Possible minds/talented people engaged
- Starting to fund the work
- Building a portfolio of assets
- We realize you are building your assets in your work, Govern will call on you to help build our collective assets
- This means we need to call on your altruistic self
- Where appropriate, ensure consistency with PG principles – Consistency Team work



2020 Key Areas of Focus

www.governforimpact.org


The materials provided by the faculty for this GOVERN for IMPACT advanced practice webinar are of a proprietary nature. Any replication of the materials or providing them to a third party without the explicit consent of the faculty member of GOVERN for IMPACT is prohibited.

GOVERN for IMPACT
Empowered Boards. Re-imagine the world...

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Building Premium Products + Services

- PG Basic Principles and Application
- Cyber Security and Governance
- Effective Ends Interpretation
- The Critical Impact of Clear Purpose
- Board Leader Character
- Effective Executive Limitations Construction and Monitoring
- Building a Board Matching Software Solution/Service



2020 Key Areas of Focus

www.governforimpact.org

GOVERN for IMPACT
Empowered Boards. Re-imagine the world...

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Building Premium Products + Services

2020 Key Areas of Focus

Govern for Impact space

Introduction / PG + Governance knowledge/skills/application

Advanced PG and governance knowledge/skills/application

[Learning, Implementation, Excellence Continuum]

Consultant/ Advisor/ Administrator space

Coaching, Consulting, Mentoring, Advocacy, Auditing Individual Boards – from implementation to sophisticated, high performing governing Boards

www.governforimpact.org

GOVERN for IMPACT
Empowered Boards. Re-imagine the world...

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Accountable PG Based Governance Training in Africa Project

- Rationale
- Concept - short (10 minute segments) x 50 (half year)
- Smartphone based, successful completion with certificate
- Targeted at millennials
- Based on PG principles and application
- Three levels – level 1 free/open source
- Levels 2 and 3 by tuition (scholarships business model)
- Govern will enter into partnership agreement
- Considering social impact investment approach



2020 Key Areas of Focus

www.governforimpact.org


GOVERN for IMPACT
Empowered Boards. Re-imagine the world...

Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Accountable PG Based Governance Training in Africa Project

We will need PG + Governance content and pedagogy experts.

Please contact me if you are interested
Also we will contact you



2020 Key Areas of Focus

www.governforimpact.org

The materials provided by the faculty for this GOVERN for IMPACT advanced practice webinar are of a proprietary nature. Any replication of the materials or providing them to a third party without the explicit consent of the faculty member of GOVERN for IMPACT is prohibited.



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Building our Network/Engaging People

Ways to Engage You – theory of the best minds in this field


- Be part of our community by being an affiliate
- Serve in our volunteer network
- Present in our introductory and advanced learning programs
- Get engaged in our ‘world of governance conversations’

Help! Need a Hubs Team Leader



2020 Key Areas of Focus


www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Building our Network/Engaging People

- Board Matching Program Coming – International
- Sound Media Presence Increased [Facebook Ads]
- Engaging more affiliates, more GSP, more contacts in the work, i.e. Build our volunteer network
- Continue to clarify roles
- Need Team Leader for Hubs



2020 Key Areas of Focus

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020


Research, Discovery, New Knowledge

- First pre-pilot research project coming to conference
- Working Group on the Future of Governance
- Future World Forum on Governance Excellence
- Supporting next research step for Govern and other research projects



2020 Key Areas of Focus

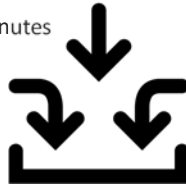
www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Seeking Your Input on Value

- Join ownership linkage session with Govern board
 - March 14th, 2020 11AM-12:30PM
 - Email Karen Fryday-Field or Kathy Wiener to join
- Complete feedback form on GOVERN’s value in just a few minutes
- Request a feedback phone call with the CEO
 - kfryday-field@governforimpact.org
- Join a team and dig your oar in!



2020 Key Areas of Focus

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Next Advanced Practice Webinar

www.governforimpact.org



Advanced Practice Webinar
Decoding Cyber & Board Governance
March 10, 2020

Karen Fryday-Field, CEO
GOVERN for IMPACT
E: kfryday-field@governforimpact.org



www.governforimpact.org