AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

FROST & COMPANY, P.S.

Spring 2016
Frostco-cpa.com

QUARTERLY INSIGHTS

Elevating Cybersecurity: Questions Boards Should Be Asking

The board's role in the oversight of organizational risk is increasingly complicated by cybersecurity concerns. Directors need to maintain continual knowledge about evolving cyber issues and management's plans for allocating resources with respect to the preparedness in responding to cyber risks. Such knowledge helps boards assess the priority-driven and investment decisions put forth by management needed in critical areas.

We have prepared the following compilation of critical questions that boards and management should be considering with respect to mitigating cyber security risk for their organizations. Questions contemplate the general to the specific, with concentrations on strategy, organizational risk profile, cyber maturity, metrics, cyber incident management and resilience, and continuing education. These questions may be useful as a starting point for boards to use in their discussions with and in the oversight of management's plans for addressing potential cyber risks.

General

- What are the potential cyber threats to the organization?
- Currently, do boards feel they are adequately up to speed on cybersecurity issues impacting their organizations?
- Do boards currently have the skill sets necessary to adequately address cybersecurity?
- What should the board be focused on with respect to cybersecurity?
- What is a suggested interaction model between senior management and the board for cybersecurity?
- Has the regulatory focus on the board's cybersecurity responsibility been increasing? If so, what is driving that focus?

Overall Cybersecurity Strategy

- Does the board need to play a more active part in determining an organization's cybersecurity strategy?
- What are the key elements of a good cybersecurity strategy?
- Is the organization's cybersecurity preparedness receiving the appropriate level of time and attention from management and the board (or appropriate board committee)?

CONTENTS:

CONTACT:
Frost & Company, P.S.
P.O. Box 7609
Olympia, WA 98501
(360) 786-8080

Frost & Company, P.S.
2412 North 30th Street
Suite 201
Tacoma, WA 98407
(253) 272-1555
www.frostco-cpa.com

- How can management and the board (or appropriate board committee) make this process part of the organization's enterprise-wide governance framework?
- How can management and the board (or appropriate board committee) support improvements to the organization's process for conducting a cybersecurity assessment?

Risk Assessment: Risk Profile

- Is the organization a direct target of cyber-attacks?
- What do the results of the cybersecurity assessment mean to the organization as it looks at its overall risk profile?
- What are the organization's areas of highest inherent risk?
- Is management updating the organization's inherent risk profile to reflect changes in activities, services, and products?

Risk Assessment: Cyber Maturity

Oversight

- Who is accountable for assessing and managing the risks posed by changes to the business strategy or technology and are those individuals empowered to carry out those responsibilities?
- Do the inherent risk profile and cybersecurity maturity levels meet management's business and risk management expectations? If there is misalignment, what are the proposed plans to bring them into alignment?

Cybersecurity Controls

- Do the organization's policies and procedures demonstrate management's commitment to sustaining appropriate cybersecurity maturity levels?
- What is the ongoing practice for gathering, monitoring, analyzing, and reporting risks?
- How effective are the organization's risk management activities and controls identified in the assessment?
- Are there more efficient or effective means for achieving or improving the organization's risk management and control objectives?

Threat Intelligence and Collaboration

- What is the process for gathering and validating inherent risk profile and cybersecurity maturity information?

External Dependency Management

- What third parties does the organization rely on to support critical activities?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?

Cybersecurity Metrics

- How should a board obtain IT metric information?
- Who should deliver IT metrics?
- What should IT metrics contain? In what format should it be presented?
- Is the information meaningful in a way that invokes a reaction and provides a clear understanding of the level of risk willing to be accepted, transferred, or mitigated?

Cyber Incident Management & Resilience

- How does management validate the type and volume of cyber-attacks?
- Does the organization have a comprehensive cyber breach response and recovery plan?
- How does an incident response and recovery plan fit into the overall cyber security strategy?

Cybersecurity Education

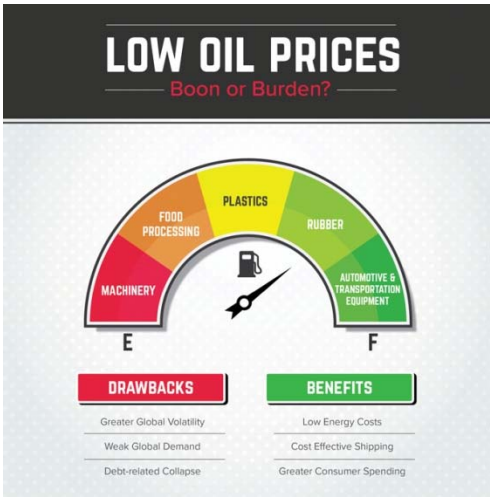
- How does the board remain current on cybersecurity developments in the market and the regulatory environment?

How Low Can They Go?

A Look at How Oil Prices Could Affect Manufacturers

It is generally believed that low oil prices are good for business and great for the overall economy. Savings at the pump give consumers greater financial flexibility and can spur increased spending, which ultimately benefits most sectors' bottom lines. For manufacturers, however, the deflated prices, which are still down nearly 70 percent from a recent peak in June 2014, have spurred nuanced effects. Some manufacturing segments like the automotive industry have benefited, while some, like the machinery sector - reliant on equipment orders from oil and drilling operations – can be financially burdened by the implications of low crude oil prices.

At the end of the day, how a company will be impacted largely depends on its product, as well as several other factors. The following infographic provides a snapshot on how a few industries could be affected and the overall advantages and drawbacks for the industry as a result of low oil prices.



Managing and Preventing Tax Related Identity Theft

Tax-related identity theft is rapidly increasing. Indeed, in February 2016, IRS identified at the top of its 2016 "dirty dozen" list of tax scams "identity theft," "phone scams," and "phishing" and reminds taxpayers of the need to guard against such scams and to protect personal information.

What is tax-related identity theft? Tax-related identity theft comes in several forms. "Identity theft," as the IRS indicates, generally involves someone stealing an individual's social security (or tax identification) number in order to file a fraudulent return claiming a fraudulent refund. Taxpayers typically discover the identity theft when attempting to e-file a tax return only to learn that a tax return has already been filed using the taxpayer's social security number. One may also learn of identity theft by receiving a letter from IRS indicating that the IRS has identified a suspicious return using the taxpayer's social security number. In many cases, the fraudulent filer claims a refund in an amount less than the payments or credits on the account, which is a flag to the IRS.

"Phone scams," according to the IRS, involve bogus phone calls from those attempting to extract undue payments from taxpayers. Victims are often threatened with arrest, deportation, and license revocation.

"Phishing" involves phony e-mails regarding fake and often unexpected tax balances due or refunds; often these include links to sham websites seeking personal information. As the IRS notes, the agency "will never send taxpayers an email about a bill or refund out of the blue."

Think You're a Victim of Identity Theft? Take Action.

PROBLEM: You attempted to e-file a return but it was rejected because another one has already been filed. **WHAT TO DO:** A paper return should be filed and should include Form 14039, *Identity Theft Affidavit*. In the case of a joint

return, one Form 14039 for each spouse and a copy of identification for *each* spouse should be included. If the e-filed return was attempted on or near the due date, the paper return should be sent within the five-day cure period (IRS Publication 4164). As always, a traceable delivery service (e.g., U.S. certified mail, UPS, or Federal Express) should be used. Thereafter, the IRS's identity theft line should be contacted at 800-908-4490 (8:00 a.m. to 8:00 p.m. local time).

PROBLEM: You received a notice from the IRS indicating a potentially fraudulent return was attempted to be filed on your account.
WHAT TO DO: Respond immediately by calling the number provided in the letter.
Important: The IRS will generally contact taxpayers only by mail. The relevant IRS letters/notices in cases concerning tax-related identity theft include:

- a 5071C letter (telling a taxpayer that the IRS received a tax return with his/her name and/or social security number and needs to verify identity),
- 4883C letter (informing a taxpayer that IRS needs more information to verify identity in order to process the tax return accurately),
- 12C letter (advising that IRS has received the tax return; however, additional information is needed in order to process the return),
- and 4310C letter (IRS Identified ID Theft Post-Adjustment Letter).

What More Can You Do?

- **Request an Identity Protection Personal Identification Number (IP PIN).** Request an IP PIN from the IRS. This is a six-digit number assigned to eligible taxpayers that helps prevent the misuse of one's Social Security number on fraudulent federal income tax returns). Upon request, the IRS will issue a CP01A Notice with the IP PIN. ***Important:*** *Currently, IP PINs are available to any victim of tax-related identification theft and any resident taxpayers of Florida, Georgia or the District of Columbia (the three jurisdictions with the highest per-capita incidents of identity theft).* IP PINs are currently issued only in January, and each IP PIN user receives a different IP PIN each January. IP PIN correspondence must be retained; they are difficult to have reissued. More information on IP PINs.
- **Request a copy of the fraudulent tax return.** A victim of identity theft, or an authorized individual, may request a redacted version of a fraudulent return that was filed and accepted by the IRS using your name and SSN. Read more on how to get your copy here.
- **Contact law enforcement.** File a police report with your local law enforcement office.
- **Report it to the Federal Trade Commission (FTC).** File a report online or by calling 877-ID-THEFT.
- **File an IRS Impersonation Scam Report with the Treasury Inspector General for Tax Administration.** Fill out the online form or call 800-366-4484.
- **Read and bookmark the following IRS materials:**
  - IRS Identity Theft page
  - *Identity Theft Prevention and Victim Assistance* (IRS Publication 4535)
  - *Identity Theft Information for Taxpayers* (IRS Publication 5027)
- **Activate a fraud alert and/or a credit freeze.** Contact the three credit bureaus and activate a fraud alert and/or a credit freeze. A fraud alert requires lenders to take extra precautions in verifying your identity before granting credit in your name. A credit freeze prevents lenders from seeing your credit report unless you specifically grant them access. To activate either one, or both, contact:
  - Equifax: online or by phone 800-766-0008
  - Experian: online or by phone 888-397-3742
  - TransUnion: online or by phone 800-680-7289

- **Be patient.** The IRS has made great strides in identifying tax-related identity theft cases and in taking early measures to assist in prevention; however, the entire process in resolving a taxpayer's account will take time. Remember also that the IRS will likely freeze any expected refund while it completes such resolution.

General Tips for Preventing Identity Theft

- Minimize personal information in purses or wallets; consider an RFID blocking wallet; retain copies of such information
- Shred any documents with personal information
- Avoid giving personal information by telephone
- Protect computers with firewalls, antivirus protection, and security patches
- Refrain from opening or clicking links to unsolicited e-mail
- Monitor accounts and review financial statements frequently
- Check that mail has not arrived previously opened
- Review credit reports frequently
- Consider an identity theft protection service

Real Estate Trends Around the World: Spotlight on Canada

Reviewing the top trends impacting real estate in an increasingly global market, BDO Canada's National Real Estate and Construction practice shares the four leading trends that are influencing the Canadian real estate market today.

Consumers are Pulling Back on the Purse Strings

Consumer debt in Canada has surpassed that of the United States. Spending on the lower end has dropped as consumers have shied away from the excess they may have embraced a few years back. That said, there is a prevailing wind of cautious optimism, mirroring what's being seen in the U.S. economy.

Foreign Investors Capitalize on the Deflated Loonie

Despite concerns that Canada could be facing a real estate bubble, foreign buyers are willing to pay a premium for in-demand properties, and we could continue to see more inbound money. China remains the top player, but we're also seeing significant investment from the Middle East.

Millennial Preferences are Reshaping Real Estate

Millennials' growing preference for multifamily urban living that caters to the live-work-play mindset is leaving its mark on Canada's residential real estate market. It is also impacting office space: as more people gravitate back toward urban markets, so do the employers that once inhabited suburban office parks.

How Low Can They Go? Oil Prices Bring Mixed Impact

In major markets like Toronto and Vancouver, low global oil prices are creating ripple effects reaching across the broader economy. But overall, low oil prices are benefitting most industries, as is the case in the United States. Also similar to the U.S. is the effect of low prices on boom towns that over-constructed to accommodate the influx in oil sands workers before prices crashed. For example, Alberta, historically heavily oil-driven, is experiencing double-digit vacancies.