ISSUE 7 | AUG 22, 2018

IIA INDIA QUARTERLY

CONTENT

In 1950, Alan Turing setup a test for determining machine intelligence, whereby on an exchange of text messages,a human attempts to distinguish between those sent by human and those by computer and if the human evaluator is unable to distinghuish, the computer is said to have passed the test of machine intelligence. Since then and over the last seven decades, the "Turing Test" was the default benchmark for determining artificial intelligence. However recently, Vinton G. Cerf the co-founder of TCP/IP protocol suggested "Turing Test 2" with a different objective in mind, viz. Cyber Security, where a computer program undertakes textual interactions with a human and another computer and if able to distinguish between these two, then passes this test. We use daily a form of this test, viz. CAPTCHA (Completely automated Public Turing Test to tell Computers and Humans Apart). This is aimed at preventing the threat arising out of a malacious program, for e.g. risk of registering millions of fake identities on an email system or making comments/spewing fake news on social media web pages or conducting denial-of-service attacks,etc.For Cyber risk to be given such a status as naming the test after Turing by one of the pioneers of the internet, surely establishes its significance and overides all other threats in the coming years. A forward looking GRC entity would surely make cyber resilience a central theme. IIA India is advocating awareness of digitial environmental risks and preparedness. In his first President's Communique, the incoming President, S. Bhaskar mentions the impact of technological innovation and digital advances on the internal audit profession, which is creating a new landscape of risk & control, and the need of internal auditors to understand these trends and leverage the use of these digital tools. Also the theme of the upcoming Delhi Chapter Annual Conference, is on digital technologies, viz. ***Staying relavant in Automation, Compliance and Technology Landscape - the time to act is now***. A training program on ***Cybersecuriity Auditing in an Unsecured World*** has been launched and the training dates in different chapters are on the website. Also a series of articles on internet risks and its management will be carried from this issue onwards, starting with Dinesh Bareja's article Business Email Compromise. This issue also contains, NG Shankar's article which brings out the current recognition of internal audit in India, its role in an entity's risk governance and the ingredients required for making internal audit effective in an organisation.

I look forward to your letters and comments.

With Best Regards

Deepak Wadhawan FCA,CPA,CIA
Editor, IIA India Quarterly
email: dwadhawan@iiaindia.org

President's Communiqué

Dear All,

Greetings!!!

"A beginning is only the start of a journey to connect another beginning."

It is an honor and privilege for me to serve as IIA India's President for the term 2018-19. I would like to first convey my sincere thanks to all my Colleagues in the IIA India National Council and the Chapters for reposing trust & confidence in me. I also take this opportunity to extend my warm wishes to all my professional colleagues and also to all the stakeholders of the profession of Internal Auditing.

Technological innovation and changes in regulatory environment are having a profound impact on the internal auditing profession. Digital advances and transformation in areas such as mobile and cloud computing, automation and artificial intelligence are transforming the way companies are doing business and thus creating a new landscape of internal controls and risk management. Internal audit must understand these trends and leverage the digital tools and technologies and integrate the same to become an agile and responsive internal audit function.

"*Emphasize the Basics. Elevate the Standards*" is the theme of current IIA Global Chairman Naohiro Mouri, and this theme is extremely relevant for IIA India. As Internal Auditors we need to first and foremost constantly emphasize on the basics in terms of *Purpose-Service- Impact*" of the Internal auditing profession. Purpose, means driving the Mission of Internal Auditing by leveraging the IPPF (IIA's International Professional Practice Framework) to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. Service means putting the purpose into action with the aim to serve the organization and stakeholders. Impact, is the ultimate outcome of the Purpose and Service in the form of the transformation, Internal Auditing and internal auditors bring about in the organization. As members of IIA, we must constantly elevate the Standards issued by the IIA. The Standards are principle-focused and provide a framework for performing and promoting internal auditing. The Standards are mandatory requirements consisting of Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance. The requirements are internationally applicable at organizational and individual levels.

In order to drive the above theme and other IIA India strategic initiatives in 2018-19, various committees have been constituted such as Conferences and Events, Training, Publications, Newsletters, Webinars, CIA Coaching, QAR, Advocacy (Public Sector & Private Sector), Institute Relations, and Membership Services including Website & Portal.

I welcome Mr. Nikhel Kochhar, the new CEO of IIA India & would like to place on record our appreciation for Mr. Deepak Wadhawan, the first CEO of IIA India who took lead in several pioneering initiatives for IIA India.

I will request all the members to actively participate in the IIA activities, in the form of volunteering for furthering the institute's goals, participating in the events, forums and conferences, promoting memberships, embracing the Standards and taking up /advocating professional certifications to further enhance the quality of our profession.

Wishing you all great success in your professional endeavors.

With best wishes,

S Bhaskar

President – IIA India (18-19)

INTERNAL AUDIT

A KEY ELEMENT OF ORGANIZATIONAL GOVERNANCE

In the present business and regulatory environment, the role and responsibilities of the Board, its Committees and Executive Management are onerous. The importance of managing investor expectations, developing a sound business strategy with high quality execution coupled with robust systems, processes and good corporate governance practices cannot be overemphasized.

Internal Audit- Statutory provisions

In February 2000, the Securities and Exchange Board of India implemented the recommendations of the Kumar Mangalam Birla Committee on Corporate Governance and inserted Clause 49 in the listing agreement. It recognized the growing importance of Internal Audit in the governance structure and spelt out its relationship with the Audit Committee of the Board of listed companies. It is now more comprehensively replaced by SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.

Section 138 of the Companies Act, 2013 requires the board of a company to appoint an internal auditor. The prescribed rules covers a) all listed companies, and b) other public companies and private companies on the basis of threshold limits related to paid-up capital, revenues, borrowings or public deposits. This has recognized the profession of internal auditing.

Role of Internal Audit

Internal Audit plays a critical role in protecting and enhancing organizational value. As a key element of organizational governance, internal audit has moved from a traditional financial audit or a compliance role to risk-based audit that proactively provides independence assurance, advice and insight in risk management, internal controls and governance. The internal audit activity is increasingly becoming a change agent and a business partner.

The primary role of internal audit is to provide assurance to stakeholders that enterprise risks are managed adequately, internal controls are working as intended, compliance processes are effective and governance mechanisms are robust. Internal auditors are the eyes and ears of executive management and give comfort to the Board and Audit Committee when they provide independent analysis, assurance and insight. They also highlight in a timely manner risk exposures or control deficiencies or identify areas for improving process effectiveness and efficiencies. Internal auditors keep a close watch on the business and regulatory environment and look for emerging risks.

International Standards

Established in 1941, The Institute of Internal Auditors Inc (IIA) provides internal auditors worldwide a comprehensive framework, standards and guidance, through the International Professional Practices Framework (IPPF), which facilitates professionalism and commitment to excellence. The Certified Internal Auditor (CIA) certification, which is globally recognized, is the hallmark of excellence in internal auditing.

As per the IIA "Internal auditing is an independent, objective assurance and consulting activity that adds value to and improves an organizations' operations. It accomplishes its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

Governance and Internal Audit

Organizational governance can be defined as a set of structures, processes, systems and practices established in the interest of all stakeholders. Executive management focuses on business strategy, efficient and effective operations, and sets a risk and control culture with zero tolerance for violation of the code of conduct or the company values. The key players in the governance structure of a company are the Board of Directors, Executive Management, Internal Audit and External Audit.

When all the governance players perform their role with integrity, diligence and operate in a well-coordinated manner, it promotes good governance, higher disclosures, transparency and accountability.

The Need for Internal Audit

Organizations need internal auditing for the following reasons. The internal auditors

- provide independent assurance to key stakeholders
- focus audit efforts on enterprise risks that matter
- assist executive management & the board in discharging their responsibilities
- facilitate the identification and assessment of risk and monitor how well risks are being managed by the business
- evaluate design and operating effectiveness of controls and efficiency of business processes
- play a positive, objective, forward looking, constructive and insightful role in assisting the management to achieve optimum efficiency and effectiveness in business processes.
- evaluate compliance with regulatory requirements, company policies, procedures and plans
- assist in monitoring management action plans that mitigate risk

Internal Audit effectiveness

- For internal audit to be overall effective, it should
- be independent, act with integrity, maintain high standards of internal auditing
- conform to professional internal auditing standards and have a quality assurance and improvement plan
- have unrestricted access to all data, information, records, property, personnel, systems and processes.
- provide real-time and relevant assurance, advice and insight and be future focused.
- have full and free access to executive management and the Audit Committee or the Board

Even in companies where internal audit is not mandated, the Board of Directors should evaluate at least annually whether an internal audit activity needs to be established.

N G Shankar, FCA, CIA, CISA
Consultant
- Internal Audit, Risk Management & Governance

Conclusion

By making it as a requirement for all listed and certain other companies, the significance of internal audit is recognised under the Companies Act. Internal audit is one of the four pillars of organisational governance and it performs its role of protecting and enhancing organisational value, through providing assurance on existing / emerging enterprise risks,-controls,compliance, process and other activities that assist Executive Management/ Board in discharging their responsibilities. The International Professional Practices Framework (IIA's IPPF) is the global benchmark that facilitates professionalism and commitment to internal audit and should be followed. Ingredients for internal audit effectiveness include Independence, complaince to Professional Standards, Quality Assurance and Improvement Program,etc. The Board of exempt companies, should evaluate at least annually whether an internal audit activity needs to be established.

Business Email Compromise (BEC)

Introduction

Across the world corporations are adopting cutting edge technologies to keep pace, or stay ahead in the race to keep their markets and business leadership. Indian businesses, small medium or large, are no laggards and we are seeing technology adoption (and innovation) at all levels, and associated risks and threats walking in through the same door.

On a daily basis, cybersecurity incidents as credit card frauds, cybercrime, identity theft, ransomware, data loss or business shutdowns, etc are reported, causing tangible and/ or intangible loss.

When talking cyber security, usually, we imagine computer geeks working hard to get into the network and crashing our business, but there are many new-age attacks and crimes which are non-technical in nature. These take advantage of human dependence and trust of computing systems to compromise an enterprise or an individual.

One such crime takes advantage of 'normal' email usage habits to perpetrate financial fraud on the individual, or company - this attack / crime is termed Business Email Compromise (BEC) or Man-in-the-Middle Email Fraud, or CEO fraud. BEC, is operating globally, and (like most cybercrimes) is largely untraceable. BEC, as the name suggests, is a method where the criminal compromises your email communication or system, makes changes over and disappears with the money you may be receiving or paying.

As Internal Auditors, one may think that stepping into the technology realm is daunting, but it has become necessary because the survival of the organization depends on tech. It is critical to be in a position to advise clients about the pervasive and stealthy manner in which this fraud is perpetrated and ensure adequate mitigation steps are applied proactively. While one may not be 100% risk free, prevention of BEC type frauds only require the application of basic good practices which is easily advised and reviewed for compliance.

The Size of the Danger, Case Studies

This fraud is dependent on the good luck of the criminal (and saad satti of the victim) – at what stage he/she walks in or discovers your contractual (or financial) communication.

An FBI report available on the Internet Crime Control Center (IC3), provides the following statistics between October 2013 and December 2016 (as reported to the IC3 and derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions):

- Number of US and international incidents: 40,203
- Total US and international exposed dollar loss: $5,302,890,448

Companies, big or small, can be targets and would not know about it until the funds are hijacked. In April 2017, it was disclosed that Google and Facebook lost a combined $100 million to someone impersonating their server hardware supplier Quanta. In June 2017, New York Judge Lori Sattler was duped into sending $1,057,500 to a scammer posing as her lawyer in a real estate deal. In August 2017, MacEwan University in Alberta, Canada was defrauded of $11.8 million in a BEC attack impersonating a vendor of the university. The list is endless.

Much like all other cybercrimes, BEC is a great opportunity for criminals, and they have defrauded victims of more than $ 5.3 billion in the three years from 2013 to 2016 and was predicted to grow to $9 billion by the end of 2018. However,

in June 2018, having updated its statistical data, there is apparently a 136 percent increase in identified global exposed losses, logged between December 2016 and May 2018. This may bring a change in their prediction of total domestic and international exposed dollar losses to US$12.5 billion (way over their own prediction or $9 billion earlier).

While there are no official figures of the size of the crime in India as the National Crime Records Bureau is yet to classify cybercrimes; one finds that practically every cybercrime investigator (private / police) has handled a number of cases. A glimpse of a partial case list of one investigator shows the details of 14 cases over two years totalling Rs. 5.97 cr ($ 865,000):

One only needs to do basic extrapolation to arrive at a rough estimate of the size of this fraud in India; considering that the above-mentioned figures are a partial list from one investigator in the country.

However, there are many cases which are reported in the news and each provides disturbing information about the varied modus operandi and the size of defrauded amounts involved:

Date	Victim	Amount Rs. (cr)	Comment
2015	ONGC	147	It was reported that ONGC was to receive a payment of Rs. 197 cr from Saudi Arabia based Aramco for supply of naphtha. Aramco paid the amount against a communication from patel_dv@ognc.co.in whereas the correct email at ONGC was patel_dv@ongc.co.in https://www.huffingtonpost.in/2015/10/14/ongc-scam-email_n_8292810.html
2018	Mumbai based	1.38	US Based client of the business man was duped into sending the payment.
			https://timesofindia.indiatimes.com/city/mumbai/south-mumbai-businessmans-us-client-loses-rs-1-crore-in-mail-con/articleshow/63776898.cms
17-Jun-18	Mumbai based company	0.1	Email asking for transfer of funds. https://timesofindia.indiatimes.com/city/mumbai/firm-loses-rs-10-lakh-as-staff-takes-orders-from-fake-email-id/articleshow/64619144.cms

As my firm undertakes IT and cybersecurity investigations, there are a number of cases handled, and the following are a few notable mentions of cases handled:

Date	Location	Amount	Comment
2015	New Delhi	Rs. 1.5cr	Garment exporter did not receive payments for 3 or 4 shipments which was paid by US based importer into the account of the fraudster. The emails of both parties had been spoofed.
2017	Dubai	$250,000	Law firm acting on behalf of their clients have to receive the amount from an arbitration settlement. Fraudster sent changed instructions on company letterhead duly signed and with company stamp.

Deconstructing the BEC Compromise

The BEC fraud has the following actors –

1. You the victim (myself.com)
2. Your customer or supplier (otherparty.com)
3. The attacker / fraudster / criminal (Mr Devious)
4. A domain registration company (where the fraudulent domains are purchased)
5. A domain Privacy Service provider (to make the fraudulent domains anonymous)
6. An obliging bank in an unfriendly / foreign country (Bad Bank)
7. Money mules or money laundering ecosystem (who get paid for passing thru')

The fraud is perpetrated silently, the fraudster having sneaked in, will keep watch on your activities over a long period of time, until a transaction is identified and compromised.

First the attacker has to get into your computer network.

Using various social engineering methods (phishing, infected USB / website / document) the compromise is carried out and a path created into the any system, or mail box of a key person in the organization - CEO, CFO, etc. (or any user).

A spam email carrying an infected attachment

is the most common attack vector and it is critical for everyone to understand this threat, and hence NEVER click open suspicious emails. In addition to spam emails we are bombarded with SMS or Social Media messages carrying titillating communication, messages enticing us to click a link or call a number - all designed to enter and infect our system to gain unauthorized access to our network.

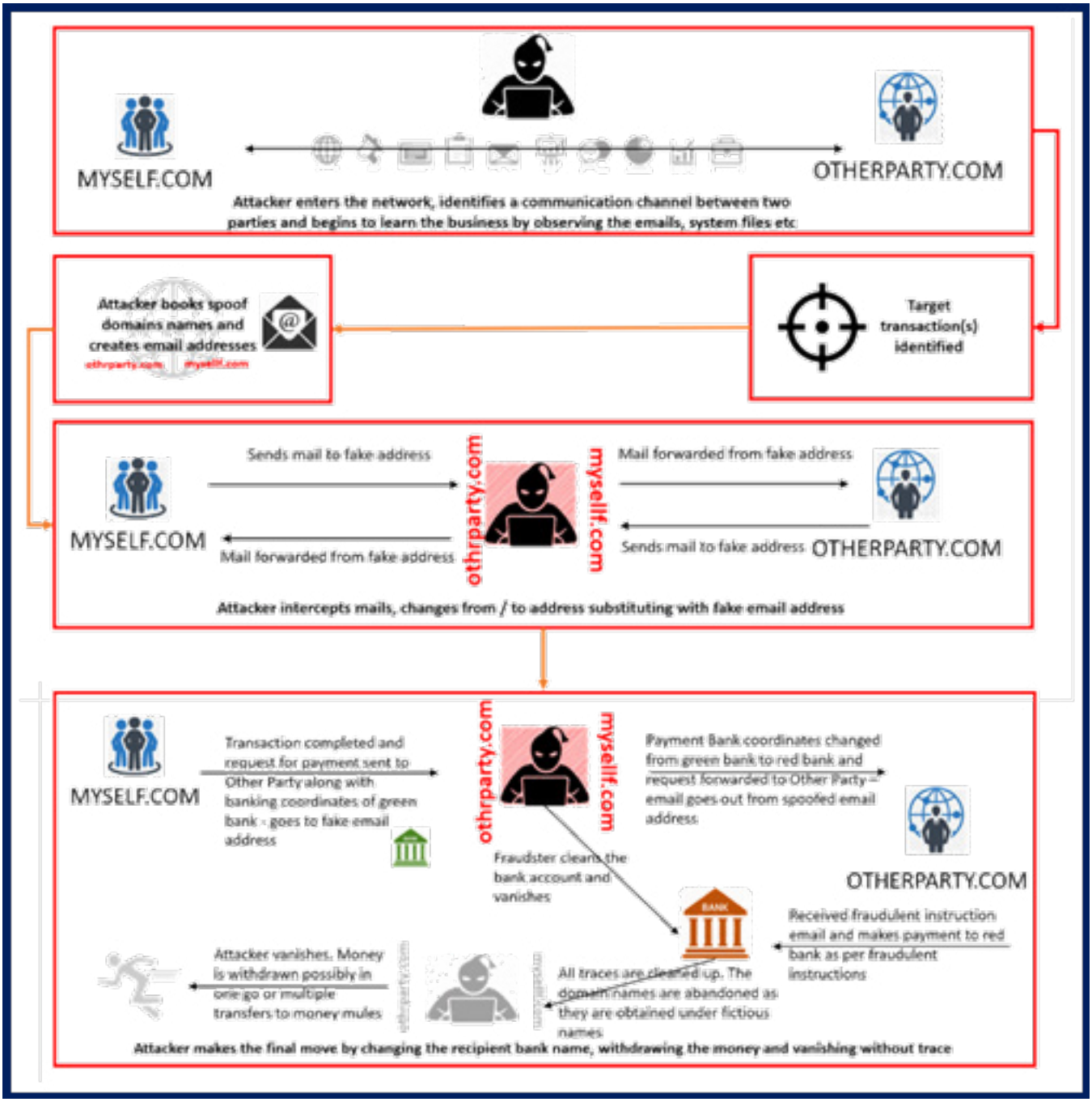
Once the attacker has entered the network the second phase is put into operation.
The criminal, Mr Devious is learning about your business, the employees, observing and monitoring activity and communication. Key-logger(s) may have been installed (a malicious program which records what you are typing and sends this to the command / control center). The settings in your email system may have been changed to forward a copy, or would have hacked into the network and have access to the internal servers. There are many other points of possible ingress by virtue of lax (or non-existent) security controls.
In short, the organization will have been mapped, to learn about the business, key persons, customers and vendors, contracts, ongoing deliveries and negotiations and more. The next step is to analyse ongoing transactions where funds can be compromised / hijacked: sales, purchase, export, import, arbitration etc.

Once the target transaction is identified, the identities (domain names) are spoofed at both ends. The domain names are usually purchased using fake names, through anonymous channels, and then a "privacy lock" is enabled so that the domain owner name is not visible.

1. myself.com can be spoofed as mysellf.com or myseif.com
2. otherparty.com can be spoofed as othrparty.com

Now begins the crime – mails sent by you from myself.com to Other Party actually start going to the fake email @othrparty.com because this fraudster has managed to make the change into the email client at both ends through a series of emails. You will remember the convenient "auto-suggest" feature of your email client whereby the frequently used email address is suggested as you type the first two or three characters of the recipient name.
This outgoing mail is received by the fraudster, who forwards it to your Other Party, after changing the from email address – [1st] the sender is changed from the original (and correct) @myself.com to @mysellf.com and [2nd] recipient is changed from fake @othrparty.com to the correct @otherparty.com.
The same act is performed for emails coming back from the Other Party, in reverse.
At this stage the fake domains become the (assumed) correct domains at both ends of the transaction and this man-in-the-middle is receiving, reading and forwarding the mails, after changing the from and to email addresses. If there are multiple addressees in the email those recipient names are also interchanged.
Mr Devious (the attacker) patiently reads mails and may make changes too, if needed, but waits until such time when an invoice is sent out or the communications fructify into a payment transaction.
The payment instruction, bank name and coordinates are changed in the final stage of the attack. Since human beings are trustworthy by nature Mr Devious' instructions are accepted and the money is transferred into the fraudulent account. Using money laundering channels, the funds are immediately moved through 'money mules' (people or organizations who rent out their bank accounts for a small percentage – they receive the money, may withdraw cash and deposit or transfer as per instructions).
The trail runs cold as the fraudster has vanished, the money has been laundered (the money mules would not know anything about the fraud to be able to provide any evidence), the domain names are abandoned and any cyber footprints and traces are removed.

A typical BEC compromise is illustrated in the graphic below:

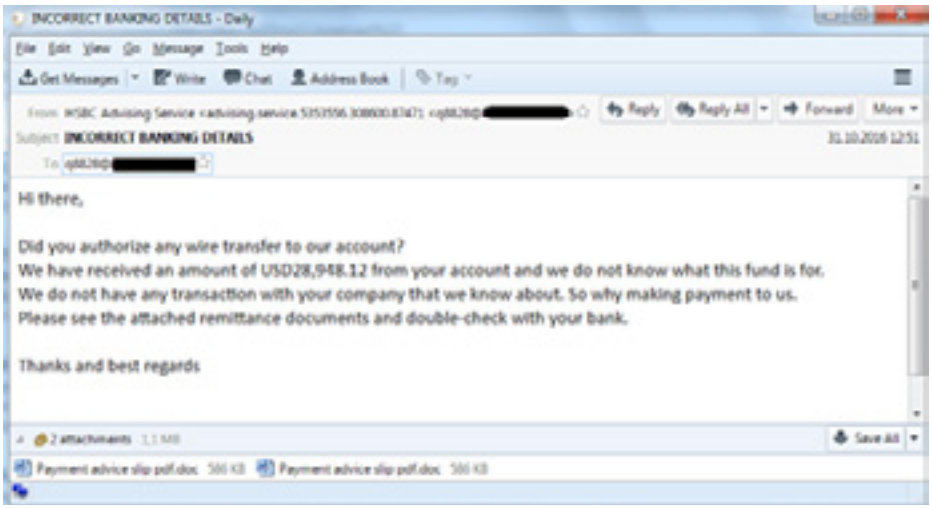


The BEC attack can be in different variants, and, notable is the CEO Fraud which uses an email account that is compromised, or a fake email is sent which is constructed to look as if it has come from the CEO. The sender field will look like "**CEO Name <ceo@myself.com>**"
This email may carry a request for a transfer of money immediately, as the CEO may have lost his/her wallet and documents, or may have been robbed or some such scenario. Flipkart got lucky:

2016	Flipkart 	$80,000 	CEO's email address spoofed and request for transfer sent to CFO – the fraud was detected and money was not sent!
	Managed to detect the fraud and did not make the transfer		https://www.business-standard.com/article/companies/flipkart-ceo-binny-bansal-becomes-victim-of-email-fraud-hackers-try-to-swindle-80-000-116031800427_1.html

However, in May 2016 Austrian aerospace parts maker FACC lost $47 million to fraudsters posing as posing as CEO Walter Stephan in an email. The Board fired the CEO and CFO. (https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF)

Then there are immediate Tax demands, Attorney demands during M&A, “out-of-pocket” expense requirement etc., or incorrect banking details as in this example email:



Source: https://media.threatpost.com/wp-content/uploads/sites/103/2017/06/06224209/incorrectbankingdetails.png

Remediation / Mitigation

If basic security hygiene practices are not have given due importance this will turn out to be the cause of disaster and, surprisingly, this risk can be mitigated substantially by the adoption of (many, if not all) the suggestions given:

1. **Awareness** – this is by far the most important activity and mostly overlooked. All users must be ‘taught’ to recognize scam emails. This can be via tell-tale signs in email signatures, writing style, language of the email, unusual account change request etc – any red flag must be escalated and investigated.
2. **Contact Creation** – when creating new customer / vendor in your ERP or payment register, make sure that the information is obtained from a business card which is in the possession of your manager(s) or CxO. Once the entry is created on your system, it must be shared with the party and with your (internal) manager, for confirmation.
3. **Email Hygiene**
   - ***Identity and uniqueness*** – the mail system can be configured so that internal emails have certain identifying characteristics which differentiate them from regular emails. Internal emails can have a different signature, background texture, font etc.
   - ***Encryption*** – sensitive emails should be encrypted or password protected. This may be an overhead, but then sensitive documents can be password protected when in transit.
   - ***Digital Signature*** – payment related emails can be signed so as to ensure the integrity of the message and will flag any tampering attempt by the fraudster-in-the-middle.
   - ***Spam Filtering*** – this must be ruthlessly enabled at the highest level.
4. **Security Audit** – must be performed regularly to confirm
   - The absence of any unauthorized forwarding email addresses or unauthorized email accounts.
   - The absence of malware or keyloggers on the company network or individual systems.
5. **Payment Processing** – any invoice or payment demand **should be restricted for transmission from a dedicated account on** a dedicated machine (if possible). The person manning this resource must ONLY type email addresses and NOT lapse into the convenience of auto-suggestion.
   - Attributes for invoices / transactions must be taken from a hard copy of the original PO or agreement.
   - Invoices or payment demands sent via email should have a follow up confirmation via fax or phone to confirm email receipt, and banking details.
   - Enable two factor authentication or have a maker checker system to confirm the recipient addresses and banking informa-

tion (in addition to the financial check on the invoice or pay out demand)

6. **Technology**
   - ***Enable DMARC*** in your email system at the very least to help prevent spoofing. While this may not be the silver bullet against the fake domain being used by the attacker, it will help set up a first line of defence. This is now a mandate from Reserve Bank of India for banks.
   - ***Use Information Rights Management*** -the IRM solution will encrypt the email and allow it to be opened ONLY by the intended recipient.
7. **Policies and Procedures** – have internal security policies and procedures along with a robust, tried and tested Incident Response and Management program.

In the unfortunate event of being a victim of the fraud you must

1. Immediately inform the recipient bank about the fraud requesting them to freeze any transaction from the criminal's account (you may need to get your own bank to enter into the communication, as the foreign bank may not consider your request).
2. File a complaint with the local police station and make copies of the same – you will need to send it to the foreign bank, your local bank, the Indian Embassy / Mission in the country where the recipient bank is located, the police authorities in the country where the recipient bank is located.
3. Your Incident response team, or Forensic Investigator, should investigate and analyse your emails to establish how and when the email address changed to the fake one and build the time line of the fraud.
4. Connect with the Other Party to obtain information about the banking and payee details, amount, email trail – build the timeline from the other perspective too.
5. Make a summary document, briefly explaining the facts and figures and send to [a] Indian Embassy / Mission, [b] the foreign bank where the money was transferred, [c] the police authorities in the foreign country – requesting their cooperation and immediate action. It will help to get a request letter from your bank addressed to each of these authorities.
6. Send a copy of this document to the Ministry of External Affairs in New Delhi asking for help.
7. Use social media resources to appeal for help and publicise all that you know about the fraudster.

Conclusion

We Are Only Human!

And, however sophisticated may be the technology deployed, there is always the risk of a failure through error, deception, accident or whatever. This has to be recognized and factored into every action planned for enabling security, but, this is easily wished upon as decision makers place higher trust in the promise of cutting edge solutions.

We also have to accept the unpleasant fact that IT / Cyber risks and threats are here to stay and one cannot wish it away, or ignore it, as someone else's domain or responsibility. This need of change of mindset applies to us, as Internal Auditors, and also to corporate management and government. In today's day and age, it is essential that audit advisory includes technology related issues and measures to mitigate the same.

A successful BEC fraud can have a significant, and material, impact on the financial health of the organization, and this is the biggest reason to be highly alert to the threat. The inclusion of mitigating controls in the financial transaction processes, internally and with external parties, will provide the safeguard against such losses.

Having said that, there is hope on the horizon with technologies like Artificial Intelligence and Machine Learning making headway to recognize attacks, but that is still to come.

Until then, email hygiene, aware and alert users, follow up and diligence in financial dealings are necessary attributes to construct a safe corporate ecosystem. While this article has focussed on the BEC risk, I may request the reader to extend his/her ambit to, by and large, cover technology risk.

Dinesh O. Bareja
Principal Advisor & Consultant,
Pyramid Cyber Security & Forensic (P) Ltd

RESOURCES FOR YOU

Mark your Calendar

August 24, 2018 – Annual conference IIA Delhi Chapter at the Grand Hotel, Vasant Kunj, New Delhi Click Here
August 24, 2018 – The IIA Hyderabad Chapter In collaboration with Hyderabad Pharma CPE Study Circle brings you a Seminar on "New Paradigm of Internal Audit" Click Here

Video Watch

2018 IIA Chairman's Message *https://www.theiia.org/sites/auditchannel/Pages/player.aspx?v=prMjM2ZjE66akNDs12hGt-d3p2EZNqq-y*
Lecture by Nawshir Mirza on Corporate Governance – Role of Internal Auditors organized by IIA Bombay & BCAS *https://youtu.be/ceBzfWTiGkU*

Internal Audit Jobs

Internal Audit Jobs - August 2018

Click Here

Chapter News

Pls volunteer at your local chapter.
For your Chapter News visit *https://www.iiaindia.org/chapter-club*

Training Programs

For IIA India held training programs visit https://www.iiaindia.org/training/training-programs

Letter to the Editor

We look forward to your letters,emails

LATEST FROM THE IIA

New! GTAG: Insider Threat Programs

Understand the insider threat universe and find new ways to improve existing insider threat programs and create new programs. This new practice guide distinguishes between malicious and non-malicious incidents and describes behaviors that may precede a threat action.

Download now.

Apply for CRMA Free in August

Earning the CRMA designation is the best way to articulate your expertise in the specialized area of risk assurance without saying a word. Don't delay - begin your application now for this distinctive certification and save up to $230 on the application.

Apply today.

New! Global Knowledge Brief on Effective Workpapers

To stay relevant, internal audit must increase its agility by pursuing quantum leaps in innovation and re-envisioning the function's capabilities. But strong internal controls will remain a foundation.

Download your complimentary copy today.

New! Tone at the Top: A Conspiracy of Silence?

In a recent survey by the National Association of Corporate Directors (NACD), 79 percent of directors expressed confidence in management's ability to sustain a healthy corporate culture. However, the survey indicated that confidence may be based on very limited information. Learn more about how the internal audit function can help assess organizational culture.

Download your complimentary copy today.

For Your Information

The IIA Welcomes Its Newest Affiliate, IIA–Venezuela

We are pleased to announce The Institute of Internal Auditors (IIA) has officially established a local presence in Venezuela! Effective June 2018, IIA–Venezuela is the official representative of The IIA in Venezuela, responsible for elevating the visibility of and advancing the internal audit profession locally.

Upcoming Global Events

27–29 August
Bali, Indonesia
IIA–Indonesia: National Conference

6–7 September
Managua, Nicaragua
IIA–Nicaragua: Regional Conference

6–7 September
Montevideo, Uruguay
IIA–Uruguay: National Conference

13–14 August
Salzburg, Austria
IIA–Austria: Annual Conference

26–28 September
Arusha, Tanzania
IIA–Tanzania: Annual Conference

27–28 September
Lagos, Nigeria
IIA–Nigeria: Annual Conference

3–5 October
Madrid, Spain
ECIIA: Regional Conference

4–5 October
Buenos Aires, Argentina
IIA–Argentina: Regional Conference

Visit The IIA's Global Event Calendar for more information.