Issue No. 21, Summer 2024

ThinkTWENTY20

The Magazine for Financial Professionals

How You Can Protect Your Organization from Ever Evolving Cyber Attacks
Ensuring Trust and Integrity in Corporate Reporting: A New Global Standard for Digital Signatures
International Clearing and Settlement and the Blockchain
The Critical Role of The Audit Committee for Internal Audit Oversight
Humanity at Work: Slow Productivity: The Lost Art of Accomplishment Without Burnout

Number 21, Summer 2024

Editor in Chief: Gerald Trites, Managing Editor: Gundi Jeffrey, Contributing Editor: Eric E Cohen

Email: info@thinktwenty30.com Telephone: (416) 602-3931

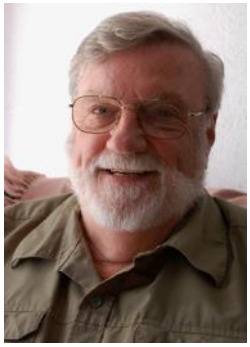
We are a community joined to learn about and discuss important issues: To join us, please go to our website at https://www.thinktwenty20.com. Regular subscription – free. Premium subscription, One year - $30, Two years - $50.

ISSN 2563-0113

Cover picture from Pixabay.com.

FOUNDING PARTNER

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA



Gerald Trites, FCPA, FCA, CISA
Editor-in-Chief

We have been publishing *ThinkTWENTY20* for five years now. That included 20 issues and almost 200 articles. In line with our strategic goals, the articles have been around 3000 words, with references, and address major issues of our times for the financial professions. A great many of those issues involve rapid change in almost everything we do, many of them driven by technology. Of course, generative artificial intelligence arrived in 2022 to start a new and fundamental set of changes - changes that promise to shake the foundations of the profession, not to mention the world.

We are proud of our little magazine and what has been accomplished so far. The articles for the most part meet or exceed our dreams of a substantial and substantive read for serious, thinking professionals. They go beyond offering helpful information to providing a grounding for thought about the issues, the profession and the direction it is taking. We are also proud of the talented professionals who have written for us over the past five years. And very grateful to them as well. They are experts and often specialists in their field.

In an age when social media style of interaction has gained an outsized role in our world, we are convinced that a magazine like ours, which provides in-depth thought content on important issues, is needed even more than ever. So you can expect to see our quarterly magazine and monthly newsletter for years to come.

Thank you for reading us!
/GDT

University of Waterloo Centre for Information Systems Security and Assurance

Table of Contents

In Their Own Words: How You Can Protect Your Organization from Ever Evolving Cyber Attacks

By Gundi Jeffrey

Gundi Jeffrey is an award-winning business journalist specializing in writing about the accounting profession for various publications in Canada and England. In 1985, she co-founded The Bottom Line, then Canada's only independent publication for the accounting and financial professions, serving as its executive editor.

As we all know by now, "cybersecurity" refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. It aims to protect individual and organizational systems, applications, computing devices, sensitive data and financial assets against various threats.

Advancements in many of the technologies we currently use have changed the way people communicate, bank, shop and pass the time. The growing threat of cyberattacks has made governments and industries more aware of the need to protect and defend the information and systems Canadians rely on. As a result, cyber security is growing as a recognizable discipline that encompasses multiple specialties in science, mathematics, business, social sciences and computing and engineering faculties. These are the folks who are going to help protect us from the scammers.

Among the many attacks we've come to know too well, are:

- **Phishing** – scammers sending fraudulent emails that resemble messages from reputable sources. Phishing attempts to trick recipients into revealing sensitive information or downloading malicious attachments.
- **Malware** – includes viruses, worms, Trojans, ransomware and spyware. These malicious software programs can infect systems, steal data or disrupt normal operations.
- **Ransomware** – encrypts files or locks users out of their systems until a ransom is paid. It has become a significant threat, with substantial financial consequences.

But there is nothing static about cyber security. Because this is an evolving field, organizations need relevant, practical advice that makes sense and helps them protect their information and IT assets. We decided to interview Janny Bender Asselin, Media Relations and Public Affairs, Canadian Centre for Cyber Security, Canada's authority on cybersecurity – which offers advice, guidance and information developed by its cyber experts – to see where these trends are heading and how organizations can best protect themselves.

ThinkTWENTY20: *Why has cybersecurity become so important? What has brought us to this place?*

Janny Bender Asselin: The pandemic brought on a rapid change in how we use technology. With so many of our everyday activities switching to online-first (shopping, work, school, etc.), the threat surface and our digital footprints increased, making it easier than ever for Canada and Canadians – both individually, and on a big or small business level – to be targets. Especially now, with many businesses depending on employees with home-based tools that might not be as secure as they would be at the office. All those different devices and service providers being added to the mix are potential new entry points for cyber criminals looking for financial gains or to gain access to a company's information.

One of the reasons so many of us are vulnerable is because cyber hygiene isn't part of our everyday vocabulary. Anyone with a cell phone, email address, social media or who browses the internet is susceptible to falling victim to a cyberattack – even the savviest cyber security expert. And keeping up with technology doesn't always feel straight forward, or it feels like it slows us down, which means the average Canadian is less likely to incorporate it. If we think "it can't happen to me" and do nothing about it, then yes, we can be very vulnerable. It's important to understand that it's no longer a matter of "if" but rather "when" we might face some form of cyber incident, and that implementing simple tools and layers of security into our day to day digital-lives makes us less vulnerable.

Our day-to-day "real life" security habits are second nature now: We don't leave our home or our car without locking the doors, so why would we leave a phone, computer or sensitive account without a strong password or PIN? We often have physical security systems in place too, so why not have multi-factor authentication (MFA) on our banking apps? It's just a new reality we need to adapt to and use some simple tools, and soon it is as second nature as hitting the lock button on a car door.

Because cyber security is an evolving field, organizations need relevant, practical advice that makes sense and helps them protect their information and IT assets.

ThinkTWENTY20: *It appears that the expanding IT landscape (cloud adoption, remote work, connected devices) provides more opportunities for cybercriminals. How do each of these developments provide those opportunities?*

Bender Asselin: All of these new connected devices are additional entry points for cyber criminals. The tools cyber criminals and threat actors use for malicious cyber activities are more readily available than ever, and at very low costs. Cyber tools that were once available only to nation-state actors, are now available to a growing set of cybercriminal organizations and other

non-state actors. This makes staying on top of cyber security, as well as new and developing threats, a challenge and a priority. We talked about not leaving the house without locking the front door, If we want to keep up with that analogy, the now tools available to cyber criminals mean that, even if the front door is locked and properly secured, they can find the basement window that was left unlocked instead. Threat actors and cyber criminals are always looking for "back door" vulnerabilities in just about every digitally connected product, and are quick to exploit them.

That's why we urge our industry partners to build in security from the start. We joined our partners across the Five Eyes alliance and beyond to advocate for information technology manufacturers to use secure-by-design and secure-by-default principles in developing their products. The guide emphasizes the need to shift the burden of cyber security risk away from the customer and instead encourage technology manufacturers to design safe products that are secure by design and by default.

Cybercriminals have shifted their tactics, placing more resources into targeting larger and more financially lucrative targets. This is called Big Game Hunting.

ThinkTWENTY20: *What are some examples of the most serious recent cybercrimes you have heard of too date? And how did they succeed?*

Bender Asselin: Though we can't comment on specific incidents, it is important to remember that all instances of cyber crime and cyber incidents are serious. Some may be a blip on the radar of a large enterprise, but the same event could be catastrophic for a small or medium organization. Every company has a different tolerance threshold, and it is important to be ready in case of the worst-case scenario whatever that may be.

In our National Cyber Threat Assessment 2020 report, the Canadian Centre for Cyber Security (Cyber Centre)'s research determined that small and medium organizations are most likely to face cyber threat activity in the form of cybercrime, which can have immediate financial,

operational or privacy implications. They often target human vulnerabilities as well as technical ones. Cybercriminals typically cast a wide net, not usually against specific targets, seeking a financial profit.

While the threat to individuals and small and medium organizations from ransomware remains, other cybercriminals have shifted their tactics, placing more resources into targeting larger and more financially lucrative targets. This is called Big Game Hunting (BGH). This means very carefully targeting large enterprises that cannot tolerate disruptions and are likely willing to pay large ransom amounts to restore their operations. Should the company not pay the ransom, they still have the company's information – which often contains personal data for individuals – which they can then turn around and sell on the dark web and still reach their financial objective.

ThinkTWENTY20: *This topic is very relevant to financial professionals, such as accountants, both in industry and in practice. What can they do to prepare for cybersecurity threats?*

Bender Asselin: In general, everyone and every organization should be aware of the basic things they can do to keep themselves as safe and secure as possible. Following our Basic Cyber Hygiene 101 for all Canadians is a great start:

1. Patch and accept updates to your software and electronic devices.
2. Practice good password etiquette. Use strong and unique passphrases or passwords.
3. Use multi-factor authentication, whenever this option is available.
4. Be on guard for phishing (and spear-phishing) messages.
5. Store your data securely and know your back-up procedures.

Since cybercriminals take advantage of technical and human vulnerabilities, the best way to safeguard your organization against the risk posed by vulnerabilities and other cyber threats is to apply cyber security best practices. While it may not be possible to entirely eliminate cyber threats, businesses and organizations can significantly reduce their risk and be better prepared by taking a few important actions, starting with:

Business leaders need to consider that their personal reputation could be at stake if their clients' information is compromised.

- **Provide security awareness training for employees**: Email phishing is the most common method that threat actors use to spread ransomware. Regardless of what security features are installed on someone's device, if a malicious link is opened, that device could be compromised. Therefore, it is important that employees know how to recognize phishing attempts and that there is a procedure in place for employees to report them to the organization's IT team.
- **Patch operating systems (OS) and third-party apps:** Unpatched and unsupported operating systems provide easy vulnerabilities for cyber threat actors to exploit. Be sure to keep your OS and all third-party apps patched with the newest updates.

- **Disable macros:** A number of ransomware strains are sent as Microsoft Office attachments. When a user opens the attachment, they are asked to enable macros to see the contents of the document. Once they enable macros, the actual ransomware payload will download and execute. Keep macros disabled by default, and make sure employees are aware that a prompt to enable macros can be a red flag.
- **Use least privilege:** Users should only have the minimum amount of system access required to fulfill their job duties. Restrict administrative privileges as much as possible, and ensure administrative users are required to confirm any actions that need elevated rights.
- **Back-ups:** Be sure to perform frequent back-ups and store them offline. If ransomware is planted on just one device, it can spread across your entire network quickly and covertly. Make sure your back-ups are not connected to the Internet or any local network.
- **Practice recovering:** Organizations should run a simulated ransomware event and practice recovery procedures. How long would it take you to get yourself back online? For many organizations, it takes a lot longer in practice than anticipated. These exercises can show you what to focus on to improve your recovery procedures.

ThinkTWENTY20: *And how can financial professionals help their clients to best protect themselves?*

Bender Asselin: Sharing resources and talking about cyber security is a great start. The Cyber Centre's website is a great resource for companies. Our "Get Cyber Safe" public awareness campaign has simple and practical information for individuals and small and medium-sized businesses, including a brand new Get Cyber Safe Guide for Small Businesses, which details the steps to take to protect your business from a wide range of cyber threats and prioritize IT security. It was created specifically for businesses without dedicated IT teams.

The vast majority of cyber incidents go unreported and that means we only have a partial picture of the impact cyber threats have on Canadians.

ThinkTWENTY20: *And which actions, of those, would be the most effective?*

Bender Asselin: As we like to say: security in layers. The more layers you implement, the better. The basics mentioned above are very easy to implement and will make a world of difference. Having MFA on an application or device may seem time consuming and cumbersome but think of it this way: recovering from a cyber incident will take far more time and money than waiting for a secondary form of identification will. Business leaders need to consider that their personal reputation could be at stake if their clients' information is compromised. That alone is probably worth taking the extra time to make sure you're using strong passwords and MFA.

Getting buy-in from all levels of an organization is very important. From the C-Suite at a large organization, to the individual who works for themselves, if everyone understands the true cost of a cyber incident – the time, the reputation, the recovery and the actual financial cost – it is easier to understand how the smaller actions you take to protect your accounts compound together to keep an organization safe. Everyone has a role to play, from the IT person to the CFO.

ThinkTWENTY20: *AI, especially generative AI, has been presented as both a threat and a possible cure in relation to threats. How does the cybersecurity centre view this topic?*

Bender Asselin: Generative AI is a type of artificial intelligence that generates new content by modelling features of data from large datasets that were fed into the model. While traditional AI systems can recognize patterns or classify existing content, generative AI can create new content in many forms, including text, image, audio or software code. While the capabilities of Generative AI present many opportunities, there are also cyber security concerns. For example, threat actors can craft targeted spear phishing attacks more frequently, automatically and with a higher-level of sophistication. The red flags for a phishing message, such as poor grammar, spelling errors and low-quality images or logos no longer apply. Realistic phishing emails or scam messages could lead to identity theft, financial fraud or other forms of cybercrime.

In a soon-to-be-published 2024 Public Opinion Research, our Get Cyber Safe campaign learned that:

- One-third (32%) of online Canadians use Artificial Intelligence (AI) tools, at home or work.
- Twenty-two percent of online Canadians reported feeling confident in their ability to recognize AI-generated content, such as messages, pictures, videos or deepfakes. An

additional 36% were somewhat confident. The rest (40%) were not confident in their ability to identify content that is generated by AI.

We all need to work together to ensure that Canadians and Canadian organizations are aware of the evolving cyber threat landscape, and how it is being altered by disruptive technologies like generative AI. We encourage Canadians to be vigilant of threats that AI platforms and apps can pose. It's also important to remember that these tools, platforms and apps may store and process information outside of Canada. Therefore, Canadians should know what information apps may request to access, and to be prudent with their privacy settings.

ThinkTWENTY20: *Your centre has urged the public to take steps to protect themselves against Ransomware attacks. How is this going? Are they taking up the challenge?*

Bender Asselin: This is very hard to quantify. We know that the vast majority of cyber incidents go unreported and that means we only have a partial picture of the impact cyber threats have on Canadians. To that effect, we encourage any organization that is experiencing a cyber incident to report it through the Cyber Centre's incident reporting webpage. Reporting cyber incidents as they happen allows the Cyber Centre to build a better understanding of the tactics, techniques, and procedures being used to target Canadian organizations. With that information, we can warn others and prevent more incidents.

ThinkTWENTY20: *How do you see this space evolving in the near future? What types of crimes can we expect next?*

Bender Asselin: In October 2022, the Cyber Centre released its unclassified National Cyber Threat Assessment 2023-24 (NCTA). This report highlights the key cyber threat trends facing individuals and organizations in Canada, and includes a section on how machine learning tools can be exploited. We highlighted that cyber threat actors are very likely exploiting new tools such as machine learning algorithms to enable malicious activity, such as the creation and distribution of e-mail fraud or phishing campaigns. In previous editions of the NCTA, we described how the technology to make deepfake videos portraying public figures or events was becoming more accessible to cyber threat actors and more convincing. In the latest NCTA, we note that we have continued to observe the evolution of the technology behind deepfakes and synthetic content and noted its use related to significant international events.

As Canadians adopt new technology and embrace more internet connected devices, the cyber threats will continue to grow and evolve. We continue to publish advice and guidance to help organizations be less vulnerable and more secure. We continue to work with industry partners to share threat information and cyber security best practices. For example, The Cyber Centre regularly publishes cyber bulletins and advice on our guidance page and urgent warnings on our Alerts page.

Ensuring Trust and Integrity in Corporate Reporting: A New Global Standard for Digital Signatures

By John Turner, LLB

John Turner is the Chief Executive Officer of XBRL International, (https://www.xbrl.org/) where he leads the ongoing development and global adoption of XBRL, the standard for digital reporting. He has been involved in the XBRL community from its outset, previously serving as the CEO of a software company, heading XBRL activities at a big four firm, and managing data collection at a prudential regulator. He is a passionate advocate for the pragmatic use of standards to enhance reporting, data availability and corporate transparency worldwide.

Corporate reports provide vital information on business performance, governing a wide range of decisions by investors, regulators, creditors, customers and other stakeholders. Reports can have an enormous impact on an organization's value and reputation. It is essential that users can trust in their integrity, with full confidence that corporate data is reliable and that audit reports are genuine. But just how solid are the foundations of that trust?

Today, users of reported financial information often lack a provable connection between a regulatory filing and its issuer or auditor. This connection is historically based on assertions by the company. Users must take reports on trust, which can leave room for manipulation by bad actors and doubt by users. To address this issue, there is a growing need to establish a higher level of digital trust in corporate reporting.

Users must take corporate reports on trust, which can leave room for manipulation by bad actors and doubt by users.

While we might reasonably consider that the risk of management manipulating an audit report before submitting it to a regulator is remote, such incidents – while rare – can have significant impact. Further, with the rise of digitization in every walk of life comes a concomitant increase in cybersecurity concerns. The risk that a corporate report (or related audit report) is manipulated by a bad actor is also relatively low, but is rising as cybercrime become more sophisticated. The impact of such a bad actor's actions, both in terms of potential loss to the issuer and on broader trust in a regulated market, could be extremely severe. It is now time, therefore, for regulators and policy makers to consider additional layers of protection.

With digital reporting now the norm in the vast majority of major markets, a digital solution to the risk of impaired trust over disclosures provided to regulators and exchanges is required. In a world where information is exchanged and utilized on a global scale, we need a global standard

for authentication. And with reporting becoming more complex and diverse – including, for example, sustainability disclosures alongside financial statements – a granular approach to authentication is increasingly important.

In this article I will discuss the need for a digital trust solution, particularly in terms of fraud prevention, and will introduce the new standard for digital signatures that is currently being finalized by XBRL International's Digital Signatures in XBRL Working Group (D6WG).

The Need for Digital Trust

The need for a digital approach to trust in corporate reporting is pressing worldwide, both to discourage and to detect fraud, as well as to ensure user confidence. The examples that follow show how fraud can occur; they are drawn from the US, but similar cases can be found in other jurisdictions. Ultimately, it is important to prevent fraudulent activities from happening in the first place, requiring a more robust and reliable connection between filings, issuers and auditors.

Here are two examples of fraud discovered by the US Securities and Exchange Commission (SEC):

1. The SEC announced that on August 6, 2001, Mark S. Jakob had been sentenced to 44 months in prison for the Emulex stock hoax and his role in disseminating a false press release that wreaked havoc with the stock price of Emulex.

Mr. Jakob was facing a loss of almost $100,000 as a result of short-selling stock in the Emulex Corporation and wrote the fake release in an attempt to cover his losses. The press release appeared to come from Emulex and falsely stated that the SEC was investigating Emulex, that the company's CEO had resigned and that the company was revising and lowering its earnings for the preceding quarter. The next day, on August 25, 2000, several news organizations republished the press release. In a 16-minute period following the republication of the fake press release, 2.3 million shares of Emulex stock were traded, and the price plummeted almost $61.00, from $103.94 to $43.00, resulting in Emulex losing $2.2 billion in market capitalization. Following a trading halt by Nasdaq, Emulex resumed trading later that day, after the hoax was discovered, and the price rebounded to close at $105.75.

Frauds, turbo-charged by the convincing inventions of Large Language Models, could be perpetrated today in all kinds of markets, and risks around cybercrime and artificial intelligence are growing.

2. The SEC filed a civil injunctive action on January 26, 2010, against Tsukuda-America Inc., an Indiana corporation, and Mr. John W. Petros, alleging fraud in connection with a $600,000 offering of Tsukuda common stock. Petros, the sole officer, director and shareholder of Tsukuda, prepared and submitted Tsukuda's Form S-1 registration statement for the offering, incorporating false and misleading statements and forged documents.

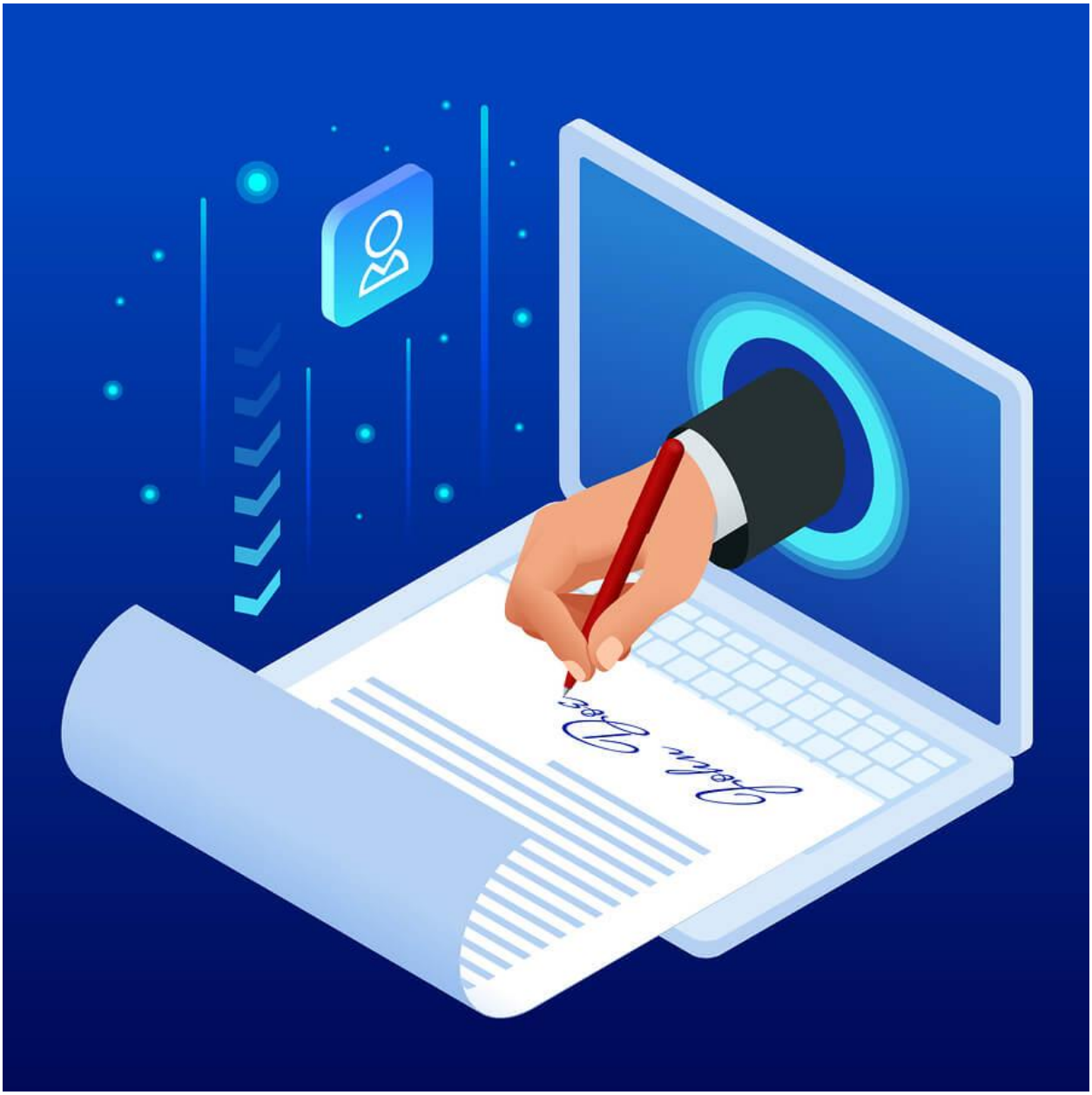
Tsukuda's registration statement contained a forged audit report, falsely identified a stock transfer agent company as the transfer agent for Tsukuda, included a bogus legal opinion and geologist's report, as well as sham consents from an attorney and a geologist who do not exist, and contained fictitious financial information.

Both of these real-life examples occurred some time ago, perhaps a testament to the work carried out by regulators in terms of authentication. It is not hard to imagine, however, that frauds of this sort, turbo-charged by the convincing inventions of Large Language Models, could be perpetrated today at scale in all kinds of markets – and that risks around cybercrime and artificial intelligence are growing.

Different regulatory environments worldwide have taken different approaches to authenticating reports. Some regulators employ only minimal security measures, while others maintain complex, multi-layered systems. A number of countries have implemented linkages between audit reports and financial statements using Adobe signatures. A rethink is needed, however, as reporting goes digital. The widespread shift to Inline XBRL, which has the huge advantage of making reports computer-readable, also means that relying on PDF signature

mechanisms is no longer feasible. The world needs an international standard for signing digital reports prepared in XBRL.

Digital signatures, applied in a standardized manner, provide the well-proven solution that regulators need. They offer verifiable proof that a document was signed by the claimed signatory, ensuring legal non-repudiation and certainty that it has not been manipulated. The cases above illustrate the ability of motivated bad actors to falsify information. The use of digital signatures could ensure that only a genuine company officer can sign a press release, only an auditor can sign an audit report, and so on, providing a clear and traceable link to each signatory. It seems highly probable that digital signatures would have prevented these cases of fraud, or ensured their detection at the time of filing.



A New Global Standard for Digital Signatures

The Digital Signatures in XBRL Working Group, or D6WG – yes, we are aware we are terrible at naming things! – brings together experts from a number of countries and is chaired by Mohini Singh of PwC. It was formed to address the global need to establish trust in XBRL-based digital reporting. The group aims to provide a standardized approach to applying digital signatures to XBRL reports.

The use of digital signatures offers essential non-repudiation, authentication and integrity in a digital reporting context. For many years, XBRL International did not have a digital signature standard on its roadmap, as it was felt there were too many national solutions, often governed by legislation unique to that jurisdiction. Cyber risks are increasing, however, and the addition of specific assurance requirements over Inline XBRL tagging decisions in the EU and elsewhere brought this question to the fore.

The focus of the D6WG is not to create a new digital signature technology. Numerous technologies already exist, including some that are legally mandated at a national or regional level. Rather, the D6WG seeks to develop consistent approaches for applying these existing signature technologies to XBRL reports.

So, what exactly are digital signatures and what do they provide? At its core, a cryptographic digital signature provides verifiable proof that a document was signed by the claimed signatory, using pairs of "keys." A private key is held by the signatory and a public one is published or otherwise made available by the signatory in a controlled manner. Thanks to the verification processes involved in the issuance of these key pairs, digital signatures prove the identity of the person signing the report by demonstrating that they possess a specific private key.

In other words, if I sign a document with my private key, then you can be confident that it was me that did so, as you can check my signature with my public key.

The proposed standard will enable companies, auditors, regulators, and other stakeholders to affirm their signoffs over a report in a digital and permanent manner.

The signing process takes as input the document and the private key, creating a very large number, which is the signature. Anyone who has the document and the public key can verify that the signature is valid – that is, that it was created using the paired private key from exactly the same document. If the document has changed in any way, the verification process will fail. Anyone who has the public key can check a digital signature, but creating a new signature requires the private key. These basic processes are 50 years old and underpin the operation of the internet, ATMs and your banking applications, as well as many other systems.

Applying this technology to XBRL, the proposed D6 standard will enable companies, auditors, regulators, and other stakeholders to affirm their signoffs over a report in a digital and permanent manner. In remaining neutral regarding the type of digital signature used, it accommodates various business and regulatory requirements. A critical feature of the standard is that it uses the fact that signatures are invalidated if any subsequent modifications are made

to the document. This ensures data integrity and facilitates data provenance, allowing users to trace the origin and history of reported information. This, in turn, enhances transparency and accountability in corporate reporting.

Another benefit of the new standard lies in its granularity. It allows for multiple signatures, linking each one to all or part of an XBRL report. A digital signature might apply to the report document as a whole, a section, a table or even an individual fact. Signatures in Inline XBRL can apply to parts of the human-readable document, specific digitally tagged facts or a combination of the two. This granularity enables multi-layered approvals, with all relevant stakeholders signing off on the appropriate parts of a report.

For example, a company CEO may sign the full annual report, while the CFO and auditor sign off on the financial report, a specialist company signs the sustainability section, the company secretary signs off the earnings release and the regulator indicates that it received the digitally signed copy at a specific time and date. This provides non-repudiation, making it difficult for any party to deny their involvement. It also makes it clear exactly where the limits of responsibility lie for each section of a complex report, and means that each signatory can put their name to just the specific content they have themselves produced or audited.

The D6WG's first deliverable was a requirements document, which outlines the necessary criteria for implementing digital signatures in XBRL reports. This was followed by a new XBRL specification, currently available as a candidate recommendation draft. One of the questions addressed by the working group was where digital signatures should be located. The specification enables signatures to be stored within an XBRL report package, so that it is securely retained alongside the report files and connected to them, without modifying the files themselves. For more on the work of D6WG, and how the new standard works with the Report Packages specification to provide a consistent solution to digital signatures in XBRL, this presentation from back in November 2023 by XBRL International's Technical Director Paul Warren is worth watching.

Digital signatures are invaluable in verifying the authenticity and integrity of a financial report and its auditors.

Furthermore, the specification allows for the use of digital signatures based on the controlled issue of "digital certificates." This requires a public key infrastructure (PKI) to issue certificates. The PKI verifies the identity of individuals receiving these certificates (strictly, private/public key pairs) ensuring that they are who they claim to be. Typically, this involves the production of an identity document like a passport or driver's license, together with a range of supporting documentation. Thus, the digital signature not only proves that the signatory had a particular key, but also that the key belongs to a verified person or entity.

In this context, the launch of the verifiable LEI (vLEI) by the Global Legal Entity Identifier Foundation (GLEIF) is expected to prove a significant development in facilitating the global adoption of digital proof of identity in corporate transactions of all kinds, including corporate reporting. The LEI is an established legal entity identifier used by companies around the world to identify themselves, including in many existing XBRL reporting systems. The vLEI is its digital

counterpart, designed for digital authentication and verification. It provides a mechanism for linking private keys to the LEI, via specific corporate roles. The vLEI is designed to permit digital proof that a specific individual holds a specific role on behalf of a specific legal entity, at a specific point in time. For example, it shows that Jane Wong is the CFO of Acme Pte Ltd, or Rohan Kumar is an audit partner at LWQH LLP.

The use of private keys that are tied to an identifier such as the vLEI makes it possible to guarantee that the document was created by the authors, audited by the stated auditors, and has not been modified since. As well as enabling traceability, this concept of "non-repudiation" ensures that the signatory cannot later deny their involvement, as the private key and signature can be verified. The only claim they can make is that their private key was stolen or accessed by someone else, something that is increasingly difficult with the application of appropriate cybersecurity measures.

Stopping Fraud in Its Tracks

Let us explore a recent example where digital signatures would have answered key questions and led to very different outcomes. A report published by Hindenburg Research in 2023 raised serious concerns about Tingo Group, a company filing with the SEC. Hindenburg Research stated that they were shorting Tingo Group because they believed the company was an obvious scam with fabricated financials. The report further highlighted that the financial statements provided by Tingo Group were riddled with errors.

Per the SEC, Tingo Group's Form 10-K for the 2022 fiscal year, filed in March 2023, reported a cash and cash-equivalent balance of $461.7 million in its subsidiary Tingo Mobile's Nigerian bank accounts. In reality, those same bank accounts had a combined balance of less than $50 at the end of the fiscal year.

What makes this situation even more intriguing is that the financial report was audited, and the auditors provided Tingo Group with a clean audit opinion. Hindenburg Research raised doubts as to whether the auditors conducted a thorough audit.

This raises two important questions: Was the report truly audited by the auditors who apparently claimed to have audited it? If it was audited, was the document the auditors saw the same as the document that was filed with the SEC, or was the report modified following the audit? Digital signatures could answer these questions effortlessly. They would have been invaluable in verifying the authenticity and integrity of the financial report and its auditors.

Digital signatures provide extremely strong guarantees that a document has not been modified in any way since it was signed.

Furthermore, the integration of the D6 standard into the report submissions process would make it highly unlikely for fabricated reports to be successfully submitted in the first place. The need for valid private keys means that it is not practically possible to generate fraudulent digital signatures or, in other words, to put a person's name to disclosures they have not willingly signed off on. At the same time, any modifications or tampering with the document after

signing would be immediately detected and cause the signatures to be invalidated, preventing submission.

What's Next?

The application of digital signatures to digital reports is a necessary step in ensuring their integrity and authenticity, and so in preventing fraud and fostering trust across today's reporting landscape. By standardizing the use of digital signatures and leveraging existing technologies, we can establish a consistent global approach to signing XBRL reports. Numerous regulators and policymakers have expressed a strong interest in the D6 specification. Once it is finalized, we anticipate that many regulators will be eager to utilize the standard.

Widespread uptake of the specification will also, however, depend on the user experience developed by software vendors, and will require user-friendly and cost-effective signing. We encourage vendors and other stakeholders to review the specification, provide feedback, and start laying the groundwork for implementing the digital signatures standard.

It is also time for a range of actors within the information supply chain to consider whether existing workflows need to be upgraded.

- Should regulators, in addition to seeking digital signatures from management and auditors over relevant sections of reports being submitted to them, *add their own digital signatures to the report?* This would provide a further guard against later

tampering by a bad actor that had gained access to their systems, as well as providing another layer of certainty about the authenticity of each corporate filing that could be relied on by investors, as well as in the course of litigation.

- Do auditors need to think about redesigning some common practices? There are situations today, in some parts of the world, in which a signed set of audited accounts are later altered by management, with the knowledge of the audit team, but not re-signed by the audit firm, not least because it might oblige the audit team to consider subsequent events. The use of digital signatures over XBRL materials would make these kinds of processes impossible.
- More broadly, we all need to consider how digital signatures will disrupt existing processes. Digital signatures provide extremely strong guarantees that a document has not been modified in any way since it was signed – and this makes it impossible to rely on being able to make minor, immaterial changes at a late stage. Digital signatures don't care whether you tripled your reported revenue or simply added a missing comma: any change will invalidate the signature. What does that mean for your practice?

We expect to see broad global adoption of the new D6 standard, ensuring trust in business data for the digital age. In a world of changing and increasingly sophisticated risks, it provides a fully digital, traceable and granular solution for report authentication and non-repudiation, facilitating fraud prevention and fostering user confidence.

We continue to seek broad inputs in order to further improve and finalize the proposed specification, which can be found here. Get in touch with us at XBRL International if you would like to be part of this process, and let's start these conversations about deploying digital signatures now.

International Clearing and Settlement and the Blockchain

By Bob Tapscott

Bob Tapscott's experience as a former board member of Payments Canada (the Canadian equivalent of the ABA) has made him acutely aware of the complexities and delays that exist in today's International Clearing and Settlement systems. His subsequent research for the Blockchain Research Institute has given him unique insights into how blockchains may revolutionize these archaic systems reducing the time to settle from days (or weeks) to minutes, while eliminating the complex time-consuming hedging now needed to mitigate risk. His thoughts more extensively can be found in his recent book - **TRIVERGENCE: Accelerating Innovation with AI, Blockchain, and the Internet of Things, 1st Edition,** *available at your favorite online book store. He is available for speeches or podcasts, on these pressing topics. He can be reached at bob@tapscott.com*

This article will be in three parts, and published in three consecutive issues. This, the first part, will explain how the legacy systems for international payments work today and from where they evolved. I know many mystified and frustrated customers that are baffled why, in the age of bits, inter-country transfers take as long as they do. Once you have read this series, you will appreciate that, when payments are in systems between countries, even your banker does not actually know where your money is. The second will explain the current projects underway to modernize these systems. The third will explain how blockchain, properly deployed could create a better system, with near immediate transfers concurrent to not just hedging but entirely eliminating risk.

Idea in Brief

The Society for Worldwide Interbank Financial Telecommunication network is a member-owned global cooperative, the world's leading provider of secure financial messaging services, and the most trusted network in the world.

The global payment system is the lifeblood of world commerce. In the Internet era, the sluggish pace, high cost, and opacity of international funds transfers, both corporate and consumer, are a source of frustration. Money seems to hang in limbo between institutions for days. Clearing a check from France to the United Kingdom within a bank that has a large presence in both countries can take six to eight weeks!

Transfers are typically based on messages sent through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network. Most banks will not respond to an international funds transfer request unless it arrives via the highly secure and trusted SWIFT network. Although SWIFT messages for the movement of funds are near instantaneous, legacy processes within the banks are not.

Emerging blockchain technologies may diminish or even replace SWIFT and the systems it supports. Distributed ledger technology (DLT) introduces three possibilities for speeding transfers and lowering costs:

- DLT obviates the need for layer upon layer of complex systems talking to complex systems to manage risk, while adding fees for their services.
- DLT enables funds transfers between countries without any significant delay.
- In DLT, trust derives from mathematics, not from "trusted institutions with their fallible humans and their legacy systems.
- As international commerce has exploded, it has demanded a lower-cost system with fewer time-consuming intermediaries. Smartphone applications will become the ubiquitous payment mechanism for the unbanked. Near- and nonbank payment systems are flourishing with and without underlying blockchains.
- This is a game changer. Consumers and corporations will know exactly when their funds will arrive and need not guess at the final currency converted amount. Payment systems for the poor without intermediaries charging high fees will stimulate greater commerce by removing friction and inefficiencies that impede greater economic purpose.
- There are two approaches in technology to implementing dramatically new systems: (1) revolutionary (the big bang) and (2) evolutionary (the invisible whisper). Almost always, a massive change implemented quickly, no matter how well planned, has unintended and negative consequences. Therefore, the transformation of trillions in international payments made daily over archaic and complex systems to DLT technology must be evolutionary.

Introduction: How the Global Payment System Works

A simple foreign exchange (FX) transaction between banks in two countries can involve many players. The traders (or their computers) agree on the amount, the exchange rate, and the future settlement date of the transaction, which (for simple spot contracts) is typically tomorrow or the day after.

For a simple case, the financial institutions involved need to ensure that the funds are on deposit and available through the central banks of those countries with the currencies involved on the date that the transaction settles. On that settlement date when both central bank clearing systems are up and running, an inter-central bank clearing system known as CLS, an acronym originally developed for *continuously linked settlement*, coordinates the near-simultaneous bidirectional transfer of funds.

If the banks involved do not have accounts at CLS, then they must go through banks that do. To those outside the system, it is about the movement of money. To those inside, it is the movement of debits and credits, with historical audit trails as secured and trusted records, through many dual-entry accounting systems. In truth, it is simply the movement of trusted and regulated bits. Yes, it is just bits.

The counterparties must trust (and accept the risk) of the banks at both ends, the clearing systems of the currencies in their respective countries, the correspondent banks and for coordination CLS. With the possible introduction of DLT, many will trust the mathematics proven to secure token movements and their messages over the trust in the many institutions (and their costs) to maintain their systems properly. Why can those tokens not be dollars or Euros? The answer is that they can be and, we will argue, soon will be.

Why the System Sometimes Doesn't Work

Despite the significant efforts (and systems) to ensure that both sides of the transaction occur simultaneously, our assumptions sometimes fail us. Consider the largest petroleum deal in Canadian history. As negotiations were ending in Calgary, the press announced that the deal was signed. Based on this, East Coast bankers transferred billions of dollars from US banks to Citibank Canada's accounts. The East Coast bankers then went home.

However, the deal was not signed. When the few who were left still working at the US banks realized that they had transferred billions with no corresponding asset (an executed sales contract), they had to convince Citibank Canada to transfer the billions back or notify the US Federal Reserve that they were technically insolvent. It was for both me and Tim O'Connell, a very long night.

Who needs risk management when we can entrust the movement of funds to irrefutable math?

Had they used a blockchain-based smart contract, whereby the terms and conditions of the contract and its execution of massive funds transfers were mathematically inseparable, there would have been no risk. Again, who needs risk management when we can entrust the movement of funds to irrefutable math? There are simple solutions to today's complexity. The original blockchain created an immutable and mathematically provable log of activity. It combined public and private key cryptography to verify identity and a consensus algorithm to verify transactions and prevent duplicate or fraudulent spending, all in a peer-to-peer network. There is no requirement for centralized control. Each feature is not revolutionary. All were available in the 20th century. The simple combination of them may well be.

Bank of England / looking up by George Rex, 2015, used under CC BY-SA 2.0.

A History of Payment Systems

Moving money between accounts within a single bank is easy. The bank simply credits one account and debits another. The consumer covers the cost of these transfers in monthly

account fees. Moving money between banks in the same country is not quite so direct. The money is redirected through that country's central bank, be it the US Federal Reserve (the Fed), the Bank of England (BoE), the Bank of Canada (BoC), or the European Central Bank (ECB). Bank automation has sped up check clearing, but banks kept most of the benefit. New systems could eliminate paper entirely. By using less paper and more bits, the clearing systems have successfully processed the dramatic rise in payment volumes.

Decades ago, most countries allowed banks to hold and, for their own profits, use their customers' funds for many days on checks drawn between financial institutions before the funds were made available to the payee. Country by country, the rules have tightened.

In Canada, the larger value transfer system (LVTS) run by the central bank settles about $160 billion a day.

For example, the US Dodd-Frank Act of 2011 required banks to make the first $200 available the day after a deposit and, if applicable, pay interest. In the Philippines, next-day availability of funds became law in 2017.

In Canada, 30 years ago, the major clearing banks would run their own check sorting machines that sorted the checks deposited according to the various banks of origin. Once a bank had completed this sorting and determined what each of the other banks owed it, it would debit those other banks' accounts at the Bank of Canada, without their prior knowledge permission. The following morning, it would return the checks to the issuing banks to verify the amounts and the accounts of the debits made.

The systemic risk was obvious; a bank in trouble could simply take (in the middle of the night) billions from other banks' BoC accounts, in effect putting them in trouble without evidence to warrant their withdrawals. Typically, if a bank does not have the funds available at the central bank, the government will act as the "lender of last resort." Governments do go to extraordinary efforts (including reserve requirements) to prevent this from happening, but it does.

In the last 20 years, most advanced capitalist countries have implemented RTGS (Real Time Gross Settlement) systems that require settlement multiple times a day. This lowers the size of each settlement to avoid systemic failures. The amount of money is massive. In Canada, the larger value transfer system (LVTS) run by the central bank settles about $140 billion a day. The retail (smaller value) system run by Payments Canada clears about $24 billion a day. In 2023, CHAPS (England's RTGS system) was clearing £91.5 trillion; on average £364.4 billion daily. Given the massive volumes of money involved, no central bank wants to implement a new system until it is proven, beyond any doubt, to be flawless.

In 2016, Canada launched a person-to-person (P2P) payment system through a bank consortium called Interac where accounts can be tied to a cell phone number or an e-mail address. Through Interac, consumers can make near-real-time payments to one another, without knowing each other's account numbers. Accepting the cell phone text message on a deposit releases the funds into the recipient's account. Although to the consumer, the payments appear to be in real time, the funds actually are transferred between the banks later in the day through the central clearing system.

Venmo in the United States offers a similar service, but without direct access to the clearing system, days can pass between the payment initiation and the funds actually arriving.[8] Credit card users pay a three percent fee, but it is free otherwise.

In the summer of 2017, the five largest US banks launched a national consumer payments network called Zelle. The expectation is that two dozen smaller banks and credit unions will join over the next year. Like Interac in Canada, Zelle in the States will provide near real-time P2P payments between consumers. To hasten its adoption, Zelle is a free service, though the bank accounts it accesses typically charge fees.

International checks issued today in one country and cashed in another can be messaged through at least two central banks, a central bank transaction coordinating intermediary called CLS (continuously linked settlement), and possibly the accounts of other intermediaries called correspondent banks (Figure 1 below). Why did this complexity evolve?

The East India Trading Company and Ronald Coase

When we buy an apple at a market, we can see the apple and the vendor can see our cash. If one party cheats, it is easy to challenge the other. When we are 10,000 miles away, that approach is not possible. How does one establish long-distance trust? Very difficult. The other party is likely subject to laws that we are unaware of and vice versa. Clearly, for the exporter, it is imprudent to manufacture and ship without seeing the money. For the importer, it is equally imprudent to pay without seeing the goods. A conundrum.

Economist Ronald Coase presented his views on why the firm existed in a lecture in Dundee in 1932, when he was just 21 years old. He argued that the firm was created and still exists because going to market for the resources was more expensive than hiring those resources internally. More specifically, the firm exists to lower transaction costs.

The search for resources, their coordination, contracting and the establishing trust was easier inside the walls of the firm. He further argued that these transaction costs tend to grow as the enterprises grew. His insights were dismissed and ignored for decades, but he was eventually awarded a Nobel Prize in 1991.

Consistent with his argument the first large-scale historical answer to the transoceanic trust problem was simply to trust oneself. Global companies arose that could buy products in one market and sell in another. No intermediaries.

One example was the Dutch East India Trading Company. It is the largest company in world history. In today's terms, it was about 10 times the size of Apple.

Its English equivalent was also massive. Originally, its main product was shipping tea from India to England. Ultimately, it found the shipment of opium from Afghanistan to China more profitable. To ensure that its version of "trust" was not violated, the governor of India raised armies that were twice the size of England's. It was not the British government that seized India at the end of the 18th century, but an unregulated company that was run by an out-of-control governor and privateer (Robert Clive). Today, he is regarded as a sociopath.

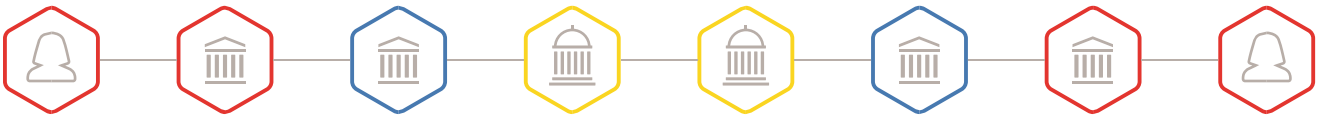
With only 35 employees in its head office in England, the English East India Company was once a model of efficiency. That was until Clive, as a rogue operative, raised and deployed an army of 260,000 without the head office's concurrence. An army was not in the company's business plan.

As Ronald Coase explained, when the transaction costs of this massive overhead (the army necessary to enforce the company's version of trust) became too large the company became unsustainable. When the English government ultimately took control of this private army, some argue it was the birth of the British Empire.

Even today, international payments pass from intermediary to intermediary in relay from sender to recipient.

Figure 1: Current Interbank Cross-Border Payment

Payer$ Recipient £



(intermediaries are called correspondent banks)

Payments between four or more parties that each trust one of the other parties that, in effect, link together for a transaction in a chain of trust. The rise of the mercantile bank, letters of credit and the associated pain.

The solve the trust conundrum emerged was the mercantile bank. It specializes and profits from managing and mitigating international trust issues between buyers and sellers that have no historical trusting relationship. Their major financial instrument to do so is called a letter of credit (LoC). This is a complex set of documents between four or often more parties that each trust one of the other parties that, in effect, link together for a transaction in a chain of trust.

If we don't trust the maker of goods, then someone we know may know someone else that they trust who trusts someone else who trusts another party, who trusts yet another someone that trusts the seller. It sounds completely unworkable, but for centuries these letters of credit were (and, largely, still are) the financial basis for international commerce.

So, for example, one bank would pay for the goods (and accept the risk) when they were manufactured to spec and available for shipment. This bank was then paid by another bank (who would then accept the transit risk) when the goods arrived and were inspected at the dock for export. This bank would then be paid by yet another bank (who would then pay and accept the next phase in the transit risk) when the goods arrived at the importer's docks. This bank was then paid by another, the bank of the ultimate buyer, when the goods arrived as ordered and inspected on the delivery dock of the purchaser. Documenting and negotiating the lengthy terms and conditions of these deals for their successful execution were slow and expensive (Figure 2 below).

For centuries, letters of credit were the grease that made international commerce possible.

The advising bank assured the seller and its bank that the buyer's bank was legitimate. Intuitively, we would expect that the time consumption and the profits of so many intermediaries in a letter of credit would grind the wheels of international commerce to a standstill. In fact, it was the opposite. For centuries, letters of credit were the grease that made

international commerce possible. Those that could negotiate these deals found them highly profitable, for the importer, exporter and all the intermediaries.

These processes, however, often failed in the negotiations of who would exactly accept what risk and when. To grease the international movement of goods, most exporter's governments would give an overriding guarantee to the guaranteeing banks through their import/export bank. Even with government backing, the "manufactured to spec" documents and the transfer of responsibilities with so many untrusting intermediate parties was a difficult but very profitable undertaking. For a bank anticipating the foreign payments of our customers is at best a guessing game that, depending on our effectiveness at playing that game, both we and our customers can win or lose. Today, to meet the foreign currency requirements of their customers, *Nostro* ("ours with you") and *vostro* ("yours with us") accounts are where banks hold their FX balances at other financial institutions.

Figure 2 – The Intermediaries Offering Guarantees In A Simple Letter Of Credit

For centuries, letters of credit were the grease that made international commerce possible. The advising bank assured the seller and its bank that the buyer's bank was legitimate. Intuitively, we would expect that the time consumption and the profits of so many intermediaries in a letter of credit would grind the wheels of international commerce to a standstill. In fact, it was the opposite. For centuries, letters of credit were the grease that made international commerce possible. Those that could negotiate these deals found them highly profitable, for the importer, exporter, and all the intermediaries.

These processes, however, often failed in the negotiations of who would exactly accept what risk, where and when. To grease the international movement of goods, most exporter's governments would give an overriding guarantee to the guaranteeing banks through their import/export bank. Even with government backing, the "manufactured to spec" documents and the transfer of responsibilities with so many untrusting intermediate parties was a difficult but, when successful, a very profitable undertaking.

For a bank anticipating the foreign payments of our customers is at best a guessing game that, depending on our effectiveness at playing that game, both we and our customers can win or lose. Today, to meet the foreign currency requirements of their customers, *Nostro* ("ours with you") and *vostro* ("yours with us") accounts are where banks hold FX balances at other institutions in other countries to cover the possible foreign currency demands of their customers. For example, for a bank with branches in, say, 10 countries anticipating tomorrow's customer demand for foreign currency in an 11th country is difficult, if not impossible. Put in too much money, and funds are wasted. Put in too little and a customer's payments may enter into an indefinite limbo. Today, international checks are temporarily held, trying to assess which are legitimate payments and which are not. This is time-consuming and, for many, results in a manually intensive reconciliation process.

All of this is a result of the lack of trust between financial institutions and their customers. Lack of trust is an overstatement, but limits on the extent of trust between banks are institutionalized. In the game of risk management, we can be right on whom to trust but still lose. Through financial markets, one can lose by trusting someone who trusts a third party that turns out not be trustworthy. This is the ultimate nightmare for all bankers. It is called *systemic risk*.

In the game of risk management, we can be right on whom to trust but still lose.

For example, in 2008, those who trusted Goldman Sachs and then trusted AIG would have been in deep trouble without the Fed's massive intervention. When there is no bank crisis conservative and libertarians state that government should not intervene in saving a failing bank. They believe it is wrong to privatize profits and socialize bank losses. History has shown, however, that there is no such thing as an atheist in a foxhole, nor a libertarian in a banking crisis. The slow government reaction to the banking crisis of 2008 seriously deepened the crisis.

What DLT could bring to the equation (by guaranteeing trust mathematically) is clearly a game changer.

The Creation of SWIFT and Its Messaging Service

Up until the early 1970s, banks sent telexes for payment instructions between countries. Though the sums of money could be massive, the processes were manual and error-prone. The instructions were in unstructured sentences, typically in English. Sometimes the intent of these messages was lost in translation. Typed and sent over telephone lines, these wire transfers were easy to lose, easy to misinterpret and easy

to hack. Math was used to detect unauthorized changes to the message, but not as extensively as it should have been.

For example, one fraudster knowing that math was used to create a secret message authentication code (MAC) that verified the from and to counterparties and the amount, simply requested a small valid "wire transfer" message, intercepted it, and then changed the currency from Italian lire to US dollars before forwarding it on, knowing that it would be accepted as an authentic message.

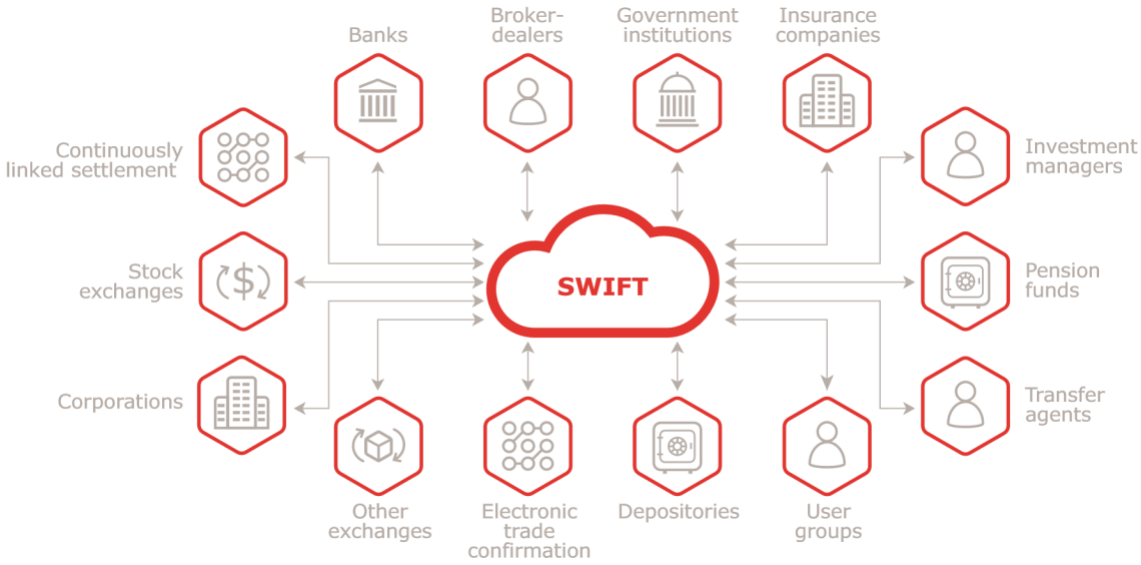
For a few thousand-dollar investment (then many millions of lire), the fraudster's return was exponential. There had to be a better way. There needed to be standards. The introduction of computers to business in the early 1970s enabled a more secure approach.

In 1973, the Society for Worldwide Interbank Financial Transfers (SWIFT) was chartered in Brussels to oversee and automate these processes. By 1978, SWIFT went online with the basic third-party controls necessary to secure financial payment messages between the larger banks and to ensure that two people at the sending institution were involved in "making and then checking" the message before it was sent and that the MAC, the pre-cursor to the digital signature, applied to all fields.

Each transfer was numbered in a sequence to ensure fraudulent insertion or deletion of messages was detected. Further standards were set for codes to indicate counterparties, currencies, dates, branches, intermediaries and action codes for a basic set of financial services. SWIFT message types have evolved beyond payments to include treasury and securities messages (Figure 3).

Figure 3: The Ubiquity of SWIFT

The Society for Worldwide Interbank Financial Telecommunication network is the world's leading provider of financial messaging services. It now has 11,000 members in more than 200 countries



Source: SWIFT (www.swift.com/about-us)

The standard for the message formats and metadata is now ISO 20022 (pronounced ISO twenty-oh-two-two).14 More specifically ISO 20022 is a harmonized set of extensible markup language (XML) financial

messaging standards, across payments, trade, securities, card and FX transactions. For changes to this standard, SWIFT is recognized as the ISO 20022 registration authority.

The Society for Worldwide Interbank Financial Telecommunication network is the world's leading provider of secure financial messaging services. It now has 11,000 members in more than 200 countries.

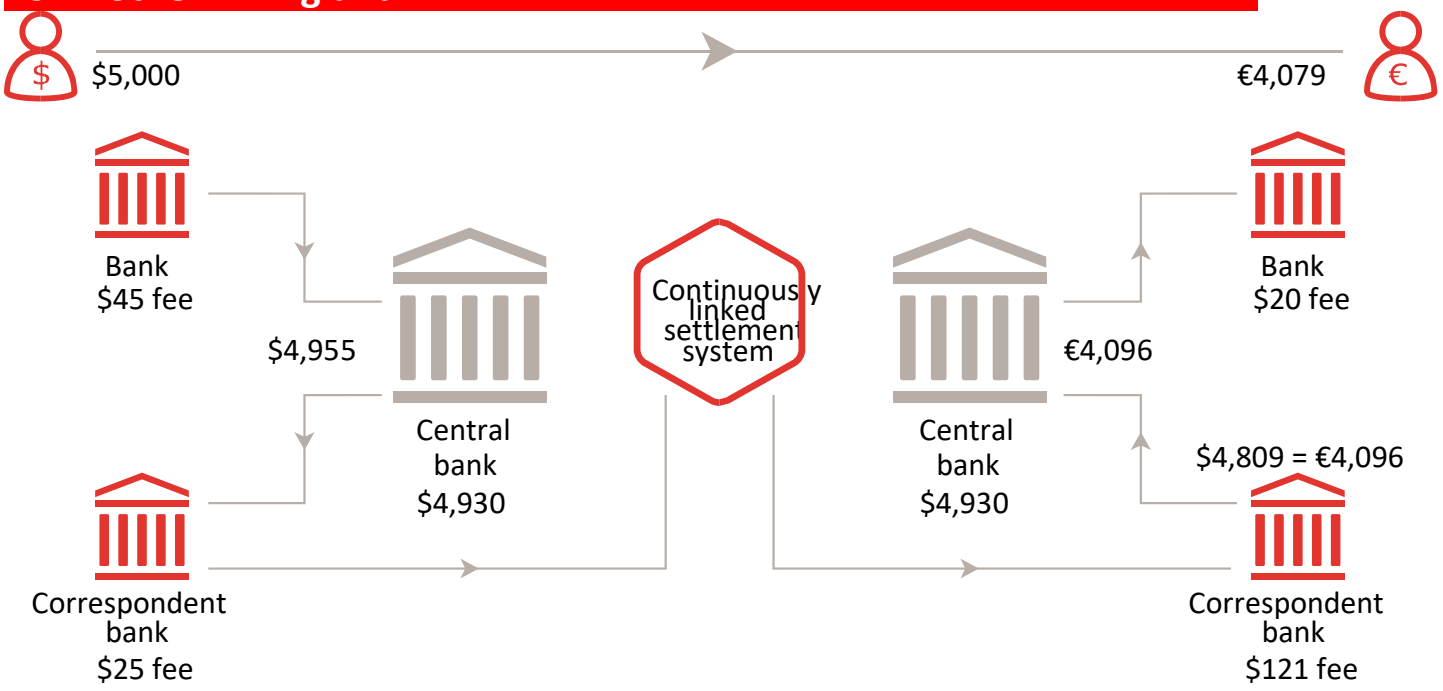
Today SWIFT sets the ubiquitous message standard, reference model, and runs the system and network for international interbank payment instructions. SWIFT is a cooperative society under Belgian law owned by its 3,000 financial institution members. It is one of the world's most trusted systems, averaging more than 27 million transactions per day. The service has expanded to include more than 200 message types including instructions for customer payments and checks, financial institution transfers, treasury markets, foreign exchange and derivatives, collections and cash letters, securities markets, treasury markets, precious metals and syndications and documentary credits. SWIFT facilitates about $150 trillion in transfers a year. That is roughly 50% greater than the planets GDP.

It is important to note that money does NOT flow through the SWIFT network.

It is simply a highly secured text messaging service for encoding, sending, receiving and then authenticating standardized structured messages from one financial institution to another. The actual movement of money typically occurs through the national clearing and settlement centers of the central banks. The timing and coordination of the movement of funds through multiple central banks and, possibly, other intermediary banks in the process makes the system slow and complex.

In a $5,000 transfer from the United States to Europe, $211 goes to the banks. Half of this sum is the difference between the mid-market rate for US dollars – Euro foreign exchange and the buy rate offered the customers. The rest constitutes fees paid to various financial institutions for their efforts.

Figure 4 – The Movement (Like Hopscotch) Of Funds From One Bank In The US To Another In England



Many financial institutions have looked at the efficiencies gained through 40 years of automation efforts as an area for more profitability, not better customer service. To illustrate, on August 23, 2024, at the TD Canada Trust site, we found that, if we converted one thousand US dollars to Canadian dollars and then back again, we ended up with $955.95. In other words, a typical bank would make ~2 percent profit in each direction on the FX conversion between two major currencies. The less significant (and liquid) the currency, the greater the loss would be to the customer because of the wider margin between the buy and sell FX rates charged.

Difficult to measure are the resulting delays in business, and the possible loss of interest in a transaction as the result of the delays anticipated. TransferWise, Venstar, OFX and other systems, although still based on fiat currencies, have discovered how to minimize the cost and the delays. Even before blockchain, the inherent inefficiencies and the profitable opportunities to disintermediate the legacy players and systems presented were compelling.

When SWIFT originally facilitated automated payments for institutions, it was primarily for large FX payments. In the 1980s, for a million-dollar cross-border payment, $50 to $100 in fees was considered acceptable. For a few personal transfers, there were always the inefficiencies of Western Union or the American Express office. With the birth of Internet commerce, however, when buying a $10 item online from China or sending money home to developing countries, $50 in fees is clearly unacceptable. The slow pace of transfers impedes commerce or could be disastrous in a family emergency. SWIFT, the central banks, traditional banks, and fintech are aware of this as a big problem, and the opportunity it offers.

The slow pace of transfers impedes commerce or could be disastrous in a family emergency.

Nevertheless, there is resistance to change. Many financial institutions have looked at the efficiencies gained through forty years of automation efforts as an area for more profitability, not better customer service. They have invested billions in these systems that they are in no hurry to write-off or discount the fees and profits they bring.

For a bank to anticipate the FX requirements of its customers correctly on a real-time basis is next to impossible. In addition, not all banks are happy about the delays and fees associated with cross-border payments. For smaller banks, having another country's currency sitting idle in its nostro accounts overseas, in case of demand, is a necessary but undesirable and unprofitable deployment of funds. For the bigger banks, however, that can act as foreign correspondents of smaller ones and that can reduce unanticipated demands by averaging over a much larger customer base, the profits are very real.

There is a lack of international standards or agreements on the speed of the movement of funds between countries. Expectations were once set based on paper-based manual systems. Inter-country regulations are typically far behind intra-country regulations. As such, there was little pressure for banks to pass on the advantages of automation to their customers. The banks looked at efficiencies gained through computerization as a source of profit, not customer service.

Nostro accounts have always been the most difficult to reconcile and the easiest to defraud. By using DLT, we might be able to eliminate the problems on nostro/vostro account reconciliation. Blockchain solutions improving end-to-end fee and rate transparency have the ability to radically disrupt this market.

Intermediary institutions between the transferor and the transferee's institutions hold and use the transferred funds for as long as possible. Today, a 30-day hold on an international funds transfer is still common. Clearing and settlement systems to avoid settlement risk may queue the funds temporarily overnight. In situations with more than one clearing system, this queue can sometimes last two or three nights. For profitable use of the funds, the banks may hold the currency much longer. Nevertheless, the consumer, confronted with an opaque process, is told that the funds are "in transit." We can track a $50 international Amazon purchase from the point of shipment to the point of delivery, yet $100,000 can hang in limbo for many days. Between countries' regulatory environments, there are few rules to protect the client, be they corporate or consumer.

Damien Vanderveken, head of research and development at SWIFT Lab and head of user experience at SWIFT, said that SWIFT is aware of the issues and has plans in place to address some of the frustrations: "If banks could manage their nostro account liquidity in real time, it would allow them to accurately gauge how much money is required in each account at any given point, ultimately enabling them to free up significant funds for other investments."

Between countries' regulatory environments, there are few rules to protect the client, be they corporate or consumer.

Very true. Nostro accounts in one country, which may be accessible by any of the bank's deposit accounts from many countries, have always been the most difficult to reconcile and the easiest to defraud. By using DLT, we might be able to eliminate altogether the problems on nostro/vostro account reconciliation.

Some of these plans are now in place. Vanderveken explained that the SWIFT global payment innovation (gpi) plans to rejuvenate the correspondent banking model by enabling a tracker feature on international payments for transparency of fees and the possibility of same day availability of funds. No doubt competitive pressures on the banks may result in a change of behavior. Then again, the status quo is so profitable, there will be much resistance to change.

Fintech start-ups that move money between countries have put pressure on the established players to be more responsive, now squeezing margins. Even when services offer nearly instant, nearly free transfers, what customers gain in speed and fees, they often lose in the exchange rate without even knowing it. Blockchain solutions improving end-to-end fee and rate transparency have the ability to disrupt this market.

Payment Systems to Manage Payment Systems

Launched in 2002, CLS is a system owned by the world's leading FX banks to address the differences in timing in settling the two halves of an FX transaction. More specifically, CLS is an international multicurrency clearing system designed to ensure that both sides of an FX contract are executed simultaneously, with certainty and with the finality of payment in two

different countries' clearing systems. The CLS system settles payment instructions of underlying FX transactions in 18 currencies through accounts with 18 countries' central banks. The technical coordination of that many banks' computers with each other in that many countries in that many time zones is not a trivial task.

The CLS system uses SWIFT messages to offer the largest FX cash settlement system in the world. Each settlement member (typically a bank) holds a single multicurrency account with CLS. At the start and end of a normal settlement day, each settlement member and each central bank has a zero balance in its account. It is not a "lender of last resort." Settlement members may submit payment instructions relating to their own FX transactions as well as the FX transactions of their third-party customers directly to CLS. CLS maintains accounts with each of the central banks whose currencies settle through CLS. CLS, settlement members and the national RTGS systems of many countries communicate via SWIFT messages.

CLS works by near simultaneously settling through the RTGS systems in the currencies and countries at times when both countries' central bank systems are open to send and receive payments. This enables concurrent settlement of the payments on both sides of an FX transaction, say, across the Atlantic. If exchanging dollars for pounds, the movement of the two currencies (dollars in New York and pounds in London) is thus coordinated in the short time window when both systems' central bank clearing systems are concurrently accessible.

Without CLS, it is probable that, in the 2008 bank crisis, FX payments would have been frozen and the Great Recession could have been far worse.

With an initial setup cost of over $300 million, CLS was criticized for its expensive structure. The cost of the cure was far (in historical terms at least) more than the disease. To the bankers, this timing difference potential problem is known as Herstatt risk. In CLS's defense, during the crash of 2008, it accomplished its primary mission of keeping FX markets liquid, when many other markets froze. Without CLS, it is probable that, in the 2008 bank crisis, FX payments would have been frozen and the Great Recession could have been far worse.

Setting up a clearing and settlement system to manage the movement of funds between clearing and settlement systems does, however, add complexity to complexity. Given the short overlapping time zones between the United States, Europe and the Far East, the flow of funds is queued and slowed. But it does accomplish its objective of managing timing settlement risk.

Although CLS's membership includes the world's largest financial players, for smaller players the indirect routing of FX transactions between organizations results in days, if not weeks of delays. Let's not forget that every private party in these transactions takes fees, and a delay of a bank taking action for a few days gives them the use of those funds for that period.

To someone outside the banking industry, all these intermediary systems may seem insane. To those with knowledge about banking systems and their history, it is perfectly logical. For bankers, each leg of the meandering journey was designed to ensure greater trust and address specific risks. As we have noted, these steps take time and money. The customer is forced to accept the delays and the costs of the overhead, as arbitrary as they seem.

More to Come…

In the next issue I will explain how different countries are updating their systems to be faster, more secure, yet still complex. I will elaborate further on how blockchains may simplify this process.

The Critical Role Of The Audit Committee For Internal Audit Oversight

by Richard Arthurs

Richard Arthurs, FCPA, FCMA, MBA, CFE, CIA, CRMA, QIAL, Partner, National Leader - Internal Audit

The audit committee plays a crucial role in overseeing internal audit and its impact on organizational operations. This article explores its various responsibilities and challenges — and provides best practices to ensure both the board and internal audit can succeed in their respective roles.

Key areas of focus include:

- The requirements for an effective internal audit charter.
- The importance of independence.
- Areas for the audit committee to assess.

We also discuss the key elements for successful collaboration between internal audit and the audit committee.

Highlights, Best Practices And Challenges For Audit Committee Oversight On Internal Audit And How It Can Impact Operations When Done Right

The role of internal audit (IA) in any organization is a vitally important one. In the complex landscape of modern business, effective governance structures which include internal audit are especially crucial to guide ethical, transparent and compliant operations.

Establishing independence and objectivity is a primary undertaking for internal auditors and the audit committee's role is to support IA to deliver value and insights in a constructive and practical way.

But how should IA and audit committees operate in tandem? Here are a few guiding principles that can ensure a smooth process while maintaining the highest levels of professionalism and responsibility.

Internal Audit Charter

In his three-part book series, *The Handbook of Board Governance*, Dr. Richard Leblanc, the keynote speaker of a 2023 event hosted by the Institute of Internal Auditors and the Institute of Corporate Directors in Saskatchewan, outlines the importance of an established IA charter.

There are several specific requirements an IA charter should have, as it relates to the function of audit committees. Here are a few of these requirements, among many others:

Purpose: The purpose of internal audit is to provide reasonable assurance to the audit committee – among other groups, including the president and CEO – in achieving internal control effectiveness over material business risks. This will come in the form of independent and objective analyses, appraisals, reports and recommendations.

Authority: The authority of the audit committee should include annual approval of the independence, mandate, resources, work plans and IA budget within the organization. The audit committee is also responsible for appointment and removal, performance reviews, compensation and succession of the head of IA (Chief Audit Executive).

Any audit committee meetings should be attended by IA and both parties should participate in an in-camera session without the presence of management.

Accountability of audit committee: The audit committee is responsible for appointing the head of internal audit, setting objectives and appraising their performance, and only the audit committee can remove the individual from that post. The chair of the audit committee is also responsible for approving the IA head's remuneration to the human resources committee.

Reporting: The audit committee should review and discuss reports produced by IA and raise any concerns of findings and management's response to those findings.

The annual plan should be presented to the audit committee at the beginning of each year for approval. In addition, a written report on IA's scope, activities and findings should be presented to and approved by the audit committee quarterly.

Internal control weakness and unresolved issues must be presented by the head of IA to the audit committee at least semi-annually to ensure risks can be reviewed and appropriate action taken.

Independence of IA

When it comes to IA independence, the role the audit committee is critical to demonstrate good governance.

For example, in-camera meetings between IA and the audit committee should not have any management present and diversity of skillset and experience within the committee is encouraged to prevent groupthink.

Internal audit can provide advisory and consulting services to management to improve risk management, governance and other control processes, as long as they are not assuming any kind of management responsibility or function in doing so.

Assessing the effectiveness of IA

To help audit committees operate efficiently and effectively, Dr. Leblanc outlines the following areas for the committee to assess as part of a holistic approach to assessing IA:

- Accountability
- Anti-fraud
- Budget
- Charter
- Compensation
- Competencies, skills
- Conflict resolution
- Coordination, coverage
- Communication
- Ethical standards
- Financial
- Independence
- Project management
- Professional development
- Quality assurance
- Recommendations
- Reporting protocols
- Resources, staffing
- Strategic
- Succession planning
- Technical acumen
- Work plan

The Five Main Elements For Success For IA Working With The Audit Committee

1. **Independence/ objectivity:** Internal auditors must operate with impartiality, free from undue influence, to provide unbiased assessments of an organization's operations. The audit committee plays a pivotal role in safeguarding this independence by championing a culture that encourages open communication and shields internal auditors from external pressures.
2. **Organizational structure:** A well-defined and strategically aligned structure ensures that IA processes are streamlined and can adapt to the organization's evolving needs. The audit committee collaborates with the IA function to establish a structure that facilitates efficient communication, delineates reporting lines, and promotes agility in responding to emerging risks, while ensuring IA is positioned at an appropriate level of authority within the organization.
3. **Adequate resources:** The audit committee plays a crucial role in advocating for and allocating the necessary resources to empower IA. This includes financial resources, personnel and other tools needed to develop an effective IA function.
4. **Management support:** The audit committee collaborates with organizational leadership to cultivate a supportive environment for IA initiatives. Management support involves recognizing the value of IA findings, acting upon recommendations and integrating IA insights into strategic decision-making. The audit committee serves as the principal liaison.
5. **Accountability and performance in accordance with charter:** A well-defined charter serves as a guiding document for IA, outlining its purpose, responsibilities, and scope of work. The audit committee plays a key role in holding IA accountable for adhering to the charter and

delivering on its objectives. Regular evaluations and assessments, conducted in collaboration with the audit committee, ensure that the IA function is aligned with organizational goals.

Compensation for the Chief Audit Executive (CAE)
Audit committee chairs might be well advised to consider structuring the compensation of the CAE differently than that of other executive management. Performance objectives might include metrics on the performance of the IA team relative to the resources devoted to it and their alignment with organizational goals.

It's important to keep in mind here that audit committees should consider the need for a different CAE pay structure while guarding against the risk of alienating IA from the rest of the organization. This could lead to problems if internal audit was seen as being rewarded for actions that lead to others receiving lower compensation.

Execution Challenges and Opportunities
There will inevitably be challenges for an organization when it comes to installing and operating the IA function. It is not uncommon for management to anticipate that IA will act in one way only to be surprised and disappointed when they do not. Rest assured; this means that IA is working correctly. There needs to be a healthy level of tension between internal audit and management.

Here are a few challenges an organization might encounter:

- **Misalignment of objectives:** Management may have specific expectations from IA that do not align with the broader objectives of the organization or the intended purpose of IA.
- **Resource constraints:** Both in terms of personnel and technology, limited resources can pose challenges. Management or audit committee expectations may not always be feasible with the existing resource allocation.
- **Resistance to change:** There may be resistance in adopting recommendations made by IA, especially if they require significant changes in processes or operations.

There are also several opportunities that can be realized with an effective and high-functioning IA team:

- **Strategic alignment:** Appropriate collaboration between IA, the audit committee, and management provides numerous opportunities to align IA objectives with strategic organizational goals.
- **Enhanced communication:** Effective communication channels between IA, the audit committee, and management fosters transparency and a shared understanding of expectations.
- **Culture of improvement:** Management's engagement with IA recommendations provides opportunities to cultivate a culture of continuous improvement within the organization.
- **Increased stakeholder confidence:** When management actively supports and values the contributions of IA, stakeholders gain confidence in the organization's commitment to

strong governance and risk management practices.

- **Balanced independence:** The audit committee can play a crucial role in ensuring that, while IA collaborates with management, it maintains its independence and objectivity.

To learn more about what a properly functioning internal audit team looks like, and how audit committees contribute to that effectiveness, contact Richard Arthurs, Partner, National Leader – Internal Audit, Enterprise Risk Services at richard.arthurs@mnp.ca, or Robert Kuling, Partner, Enterprise Risk Services, at robert.kuling@mnp.ca.

Humanity at Work: *Slow Productivity: The Lost Art of Accomplishment Without Burnout*

By Robert Edison Sandiford

Robert Edison Sandiford is the author of several books, among them the award-winning The Tree of Youth & Other Stories, And Sometimes They Fly *(a novel) and Sand for Snow (memoir). He has also written graphic novels for NBM Publishing. In 2003, he and the poet Linda M. Deane founded the Barbadian cultural resource ArtsEtc Inc. He has worked as a publisher, teacher and, with Warm Water Productions, producer. His fiction and non-fiction have appeared in newspapers, journals, magazines and anthologies. Currently working on another novel about fathers, sons and dementia, his latest book is Fairfield from DC Books.*

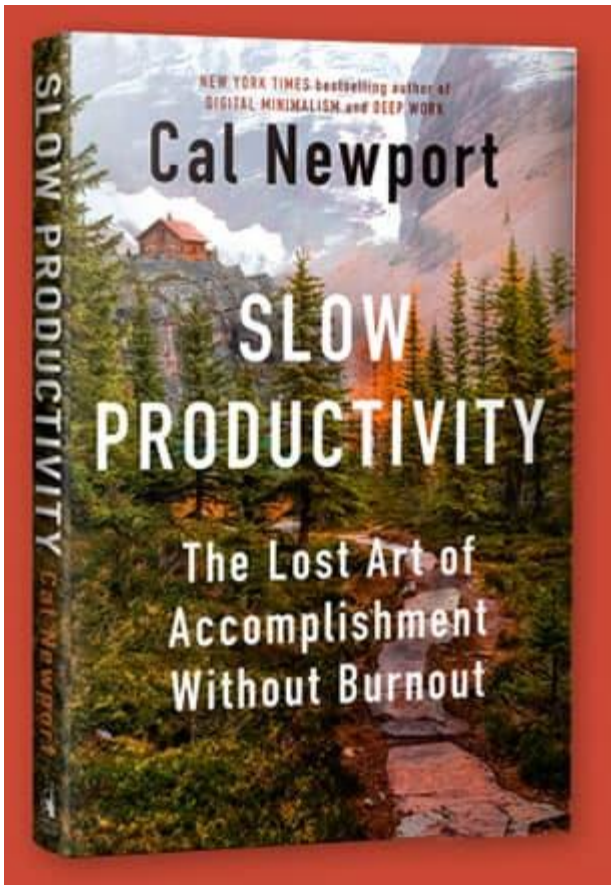
"Ten half-done jobs are not five complete jobs." **Carl Gittens, Master Plumber**

Who says the pandemic wasn't good for anything? In a world locked down by the coronavirus from 2020-2023, some of us spent our real-life Blip (as opposed to the fictional Marvel movies one) thinking of ways to live and work and even play more sanely and serenely than we hitherto had been. Cal Newport was ever one of these types, and *Slow Productivity: The Lost Art of Accomplishment Without Burnout* is a brief – overview? – distillation? – I'm not sure which word fits best – but a run-through his thoughts, feelings and philosophy with respect to what could be called a noticeable, ongoing development in the world of so-called knowledge work.

Newport's immediate past titles are telling, not just intriguing: *A World Without Email*; *Digital Minimalism*; *Deep Work*. They have increasingly examined ways for us to work smarter, not harder, and the last listed is concerned with "seeking focused success in a distracted world."

These are books that suggest a reckoning – with how we work today, how we define progress in our social spheres and also in our private lives. His current book's dedication to his family, who have reminded him of the art, the vital *necessity*, of ease, puts a fine line under his way of thinking these days.

Newport opens with an anecdote about John McPhee's writerly anxiety, or picnic table paralysis, in 1966. It is, in fact, a situation most of us can directly access, and a motif he repeats throughout *Slow Productivity* with other "teachable moments" or telling tales. I've never been



one to overcommit – but I should say no more. With the years, my work has gotten more challenging to me, if to no one else. The "fear and panic" McPhee felt over his Pine Barrens story I have felt over my next book. The upshot? We do it to ourselves: more than stress ourselves out.

According to Newport, there are some decent explanations for this behaviour. "It doesn't matter that something you've done before worked out well. Your last piece is never going to write your next one for you." Even after figuring out the way forward, "it still took McPhee more than a year to finish writing his article…."

The focus is not so much on McPhee's "fear and panic," rather on the time required to produce "a marvel of long-form reporting." What's equally significant is that Newport "came across this story of John McPhee's unhurried approach" during the COVID-19 pandemic – "a complicated time for knowledge workers." A time of great "unease" and uncertainty about "*productivity*."

A *New Yorker* contributor, blogger and podcaster, as well as bestselling author, Newport says that many of his readers during the pandemic were "*fired up*" over productivity expectations. He detected, at least in those who wrote to him or commented on his blog, "this growing anti-productivity sentiment." He further linked "[t]his exhaustion with work" to "multiple waves of heavily reported social trends…during the pandemic," such as "the so-called Great Resignation" and "the rise of quiet quitting," notably by younger workers in the West who were, to borrow the words of journalist Celeste Headlee, "overworked and overstressed, constantly dissatisfied and reaching for a bar that keeps rising higher and higher."

Newport talks about covering "the anti-productivity movement" during the pandemic, but he edges closer to his topic when he writes, "The pandemic didn't introduce this trend as much as push its worst excesses beyond the threshold of tolerability." This was loudly so for knowledge workers, whom he defines as creatives, technicians, artisans and countless others in various fields "who made a living with their minds." Going back to McPhee, whose example hangs over the narrative, Newport notes that, after 29 books, a Pulitzer Prize, National Book Award nominations, countless articles, mentoring and more, his fellow *New Yorker* contributor has indeed been productive, "and yet nothing about his work habits is frantic, busy, or overwhelming."

"The intersection of work and life needs some work," observed Jim Harter as Gallup's chief workplace scientist. What Newport proposes is that "knowledge workers' problem is not with

productivity in a general sense, but instead with a specific, faulty definition of this term that has taken hold in recent decades. The relentless overload that's wearing us down is generated by a belief that 'good' work requires increasing busyness – faster responses to email and chats, more meetings, more tasks, more hours." What Newport's after, by way of solution, is the transformation of "our modern understanding of professional accomplishment." This brings us to his philosophy of "slow productivity" and its three easy-to-remember tenets: 1) Do fewer things; 2) Work at a natural pace; 3) Obsess over quality. (Here I wonder if, by the end of the book, he will have a similar plan for us to maintain our income. But not to get ahead of ourselves.)

"Taking your time ain't laziness." **Barbadian proverb**

For people like me who have exercised what Newport advocates for most of our professional life, there is much here that is as validating as it is familiar. We *should* live the slow way. If only because we already know its benefits. We know we are just as productive during periods of calm as we are during periods of seemingly endless entropy. There may even be evidence to suggest we are more so.

Newport's goal with *Slow Productivity* is as simple as his three rules, and this is for all kinds of workers: "to…propose an *entirely new way*…to think about what it means to get things done." Personable as he is, convincing as his writing may be (the occasional overuse of "however" aside), does he succeed?

First, there are some challenges, both social and historical. A twentieth-century view of work is that "[t]he most successful companies have the hardest workers," and managers are there "to ensure *enough* work is getting done." Quantity remains king in the twenty-first century, even if quality suffers. The truth we seek, notably in the knowledge sector, is far more nuanced. Largely because how I define productivity or being productive might be quite different from how my nearest colleague does.

For me, it has to do with the amount of work accomplished in a set period of time; deadlines, and meeting them; and with maintaining the integrity of my hourly rate depending on the project. So, it's connected to meeting a budget, which then is connected to meeting my bills and balancing my budget, and that would be for home, work and play. *What* I do comes far less to mind than *how* – these days, at the age of 56. This is not the case for many others, particularly those younger than I am. In a survey Newport conducted, none of his respondents answered with "specific goals to meet, or performance measures" to determine a job well done.

And this may be because there are usually several on the go. "In knowledge work," he contends, unlike in other fields, "individuals are often wrangling complicated and constantly shifting workloads": a PR campaign along with website content along with AI training along with a poem, short story or script. "In this setting," unlike that of, say, an assembly line, "there's no clean single output to track."

The prevailing belief since the mid-1990s, with the arrival of "networked computers in the office," is that "[i]f you can see me in my office – or, if I'm remote, see my email replies and chat messages arriving regularly – then, at the very least, you know I'm doing *something*…."

But this is pseudo-productivity, asserts Newport: "[t]he use of visible activity as the primary means of approximating actual productive effort." The perpetuation of this false metric is the real roadblock to greater life-work balance, causing "significant" damage.

That's perpetuation by *us* as much as by others. As I told a colleague of mine recently who commented on how "consistent" my output was as writer/editor/publisher, "I may be more *persistent* than consistent." Some myths are useful. Lying to ourselves, especially when trying to determine an average work day and the value of the work we do today, not so much.

My usual solution when the world is too much upon me is to slow it down: reorder my schedule to reflect considered deceleration, not frenetic acceleration. It is, as Newport makes clear, my schedule to control after all, wizard-like. If this sorcery doesn't work, I'll go into quick-hit triage mode: take, maybe, five items/projects/files/jobs that need to be done in, say, a week and work *only on them*. "Our brains work better when we're not rushing," Newport reminds us. Priorities remain priorities only if we say they are and treat them as such. And it's a rather rare day in life when everything is a priority.

There are parallels here to the "slow food" movement, a term coined by "seasoned activist and journalist" Carlo Petrini circa 1986. One of its tenets: don't "confuse efficiency with frenzy." There are benefits to something developed (and enjoyed!) with an eye on "time-tested cultural innovations" versus something pushed out in higgledy-piggledy haste; one of them may be the preservation or evidence of "the human experience" in creative endeavour. There's something to be celebrated about the *space* "traditional knowledge workers [once] enjoyed" to do their job. Newport believes it is ever possible to "find in their experience the foundations for a conception of productivity that makes our harder jobs more manageable."

(Perhaps a convention of his genre, this may also be why Newport slows down his own narrative by pausing quite leisurely to describe what he will cover next. There are a number of interludes and references to work he has previously published on the topic. His pace, if not entirely unhurried, is easygoing. Do we need so much explicit foreshadowing, and does so much direct recapping of his own articles on the topic feel like padding? Not always to the first, sometimes to the second. As readers, though, we should remember not all text is to be speedread, skimmed or offered without backing reference.)

Newport admits that "those who…work in an office environment under close supervision might have a harder time fully instituting the strategies I suggest." The same goes for certain other professionals; flexibility may depend on the stage they're at in their jobs. But "the conditions for productivity," particularly of the slow kind, must first be right – as they were for another of his slow productivity avatars, Jane Austen, from about 1796-1800, and again in 1809.

A reduction in the daily busyness of her father's parsonage permitted Austen "the ability to establish the 'rhythm of work,' as [biographer Claire] Tomalin puts it" in *Jane Austen: A Life* (1997). Austen, the author of *Emma* and *Pride and Prejudice*, among other classics, didn't only gain "real and meaningful space to think and work creatively"; she gained agency, actual power over her time and how (wisely) it was spent. She may not have been frantic with *related* work, but there were the almost ceaseless demands of her family's professional and social realities to contain. On the other hand – and here we come back to budgetary considerations – "Even if

you're a solopreneur in full control of your days, the need for income might undermine your intention to reduce your workload." Few knowledge workers can count generous wealthy relatives, old-fashioned patrons or indulgent sponsors as resources.

When you've done your best, angels can't do better." **Iris Carlottie "Lots" Sandiford, My Granny**

For all Newport and others have written, for all the hirings and firings, quiet quittings and HR debates, what have we learned about ourselves in the last half decade? Anything? I find *Slow Productivity* highly relatable. Often, I wonder which lessons about our climate (remember the returning animals and clearer mountaintops?), our vulnerabilities and our strengths we've retained in our mad need to get back out there and be busy, never to be locked down again.

All workers, claims Newport, can count on themselves and their ability to change their ways and, in turn, their fortunes. Apart from banking on ourselves, he provides an arsenal of approaches to work meant to convert pseudo-productivity into genuinely transformative productivity: the kind that has the potential to change worker's lives and maybe, in the process, our societies: by leaning into practical, sensible, humane ways of work that reduce the law of diminishing returns. More work does not necessarily equal more pay or more prosperity or more achievement. It's OK to say no to a job upfront, rather than wait until it puts us in "sufficient personal distress to justify the distress saying no might generate in the other party." People are more likely to respect our time when we respect our time.

Other Newport advice: don't put money above health. Much in the same way we should avoid putting money above our integrity. Work seasonally, work to a calendar schedule or five-year plan, work only certain days a week, work a pull rather than push method, work less hours for more money, work after the kids are in bed (or with them on our lap, if quiet and small enough, I say) – whatever we choose from his many excellent tips and suggestions, find what works *for us* to be truly productive. And then commit to it. Refine it by avoiding task and admin generators that "in sufficient quantities, can act like productivity termites." All the while remembering to be gentle with ourselves as much as with clients and family. To talk instead of text; to limit our projects lists instead of expanding them. Obsessing over quality "isn't just about being better at [our] job" but being better at improving our overall circumstances. It could be nurturing a hobby or going for a regular walk. We should, as a far younger colleague advised me almost 30 years ago, work to live, not live to work.

If anything, that's what's changed for me since the pandemic. I'm older. I can spot inefficiencies more quickly. I know there's more than one beneficial way to do something, and there will always be something that needs doing. And…I'm older. With experience gained over time has come the greater, sharper knowledge that I have less time to waste or have wasted.

But then I would argue: younger or older, knowledge worker or field labourer, student or newly employed, we should all feel this way.