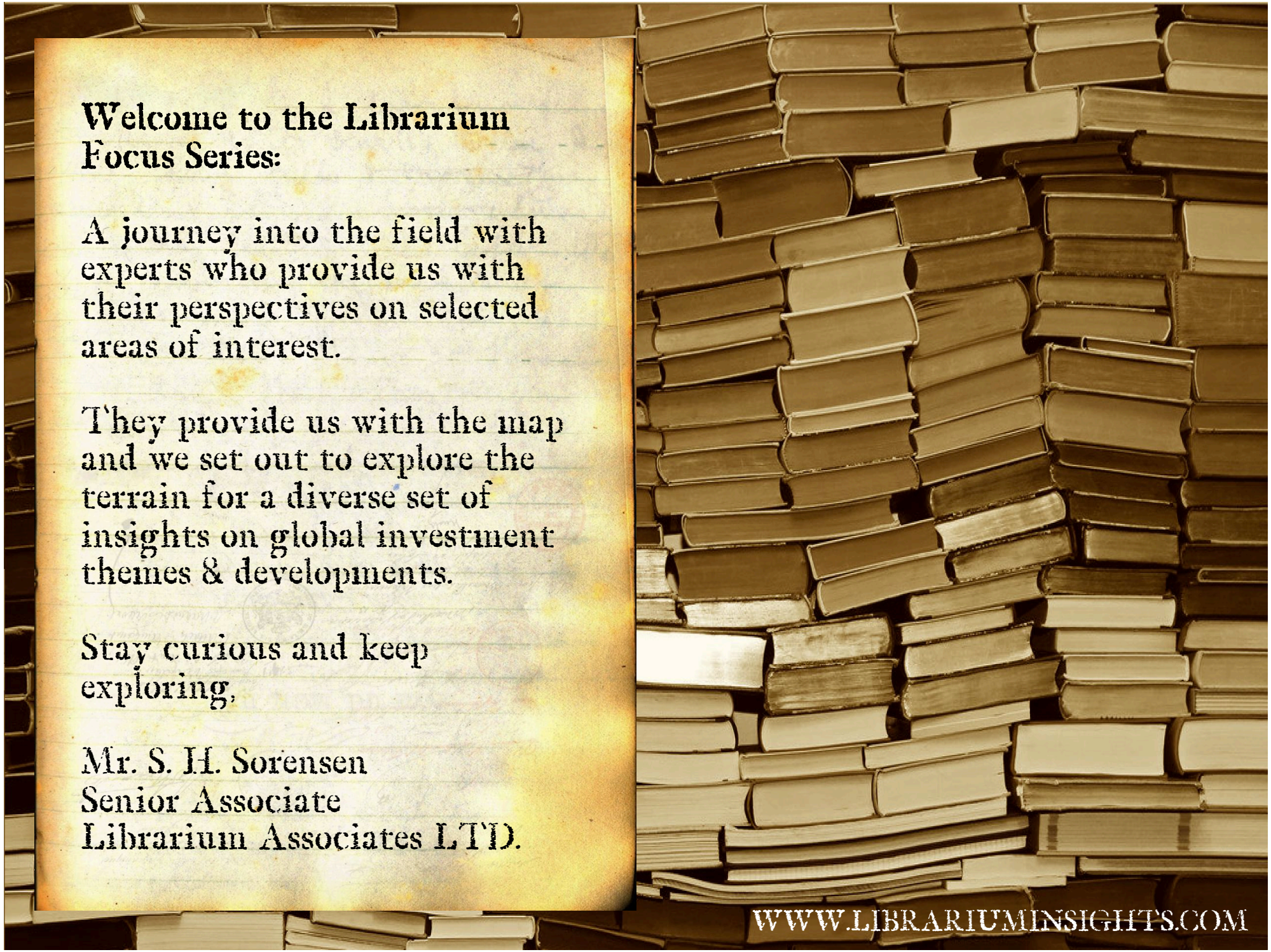
The Librarium Focus Series

A topical series where we set out to explore new perspectives with experts in the field:

A LOOK AT INNOVATION IN CYBER SECURITY WITH: ERIK KELLOGG & EDUARDO GALIANO

Volume 2 – Q3 – 2018


Welcome to the Librarium Focus Series:
A journey into the field with experts who provide us with their perspectives on selected areas of interest.
They provide us with the map and we set out to explore the terrain for a diverse set of insights on global investment themes & developments.
Stay curious and keep exploring,
Mr. S. H. Sorensen
Senior Associate
Librarium Associates LTD.
WWW.LIBRARIUMINSIGHTS.COM

MEET OUR VISITING EXPERTS...

Mr. Erik Kellogg is the CEO of inCyber Security, a leading full-service cyber security & cyber compliance consulting firm. Over the last 17 years, he has filled key technology roles within the financial industry including. Erik is a cyber security expert with a proven track record of helping businesses protect themselves from cyber threats and adhere to industry regulations.

Notably, Erik and his has developed a proprietary, data driven, cyber risk model as a way for their clients to bridge the gap and understand cyber impacts in dollars & cents, which all levels of an organization can relate to.

Erik is based in Chicago and you can learn more about his work here: www.incybersecurity.com

Mr. Eduardo Galiano advises the InCyberCompliance division of InCybersecurity. They focus on automated compliance, regulatory, risk analytics and monitoring via the company's CyberDash software.

He has advised current and former CEOs & Chairman of major commodity exchanges in North America and Asia focusing on risk management and big data.

He is a former marketing consultant and big data specialist for McKinsey & Company, Inc. He has been a director for a South East Asian commodity trading group focused on agricultural and bullion.

He has studied Cyber Security systems at MIT and Systems Dynamics under Professor Jay Forrester.

NOTICE: While we draw on our visiting expert's wisdom in these collaborative reports, we are perfectly capable of making our own mistakes and our guests should not be considered accountable for any errors or lack of understanding. We humbly try to distill insights from their expertise but at the end we navigate the journey on the quest for knowledge as to the best of our abilities.

A BIG PICTURE OVERVIEW OF OUR DIGITAL REALITY.

A look at the powerful trends at play representing both enormous opportunities and risks:

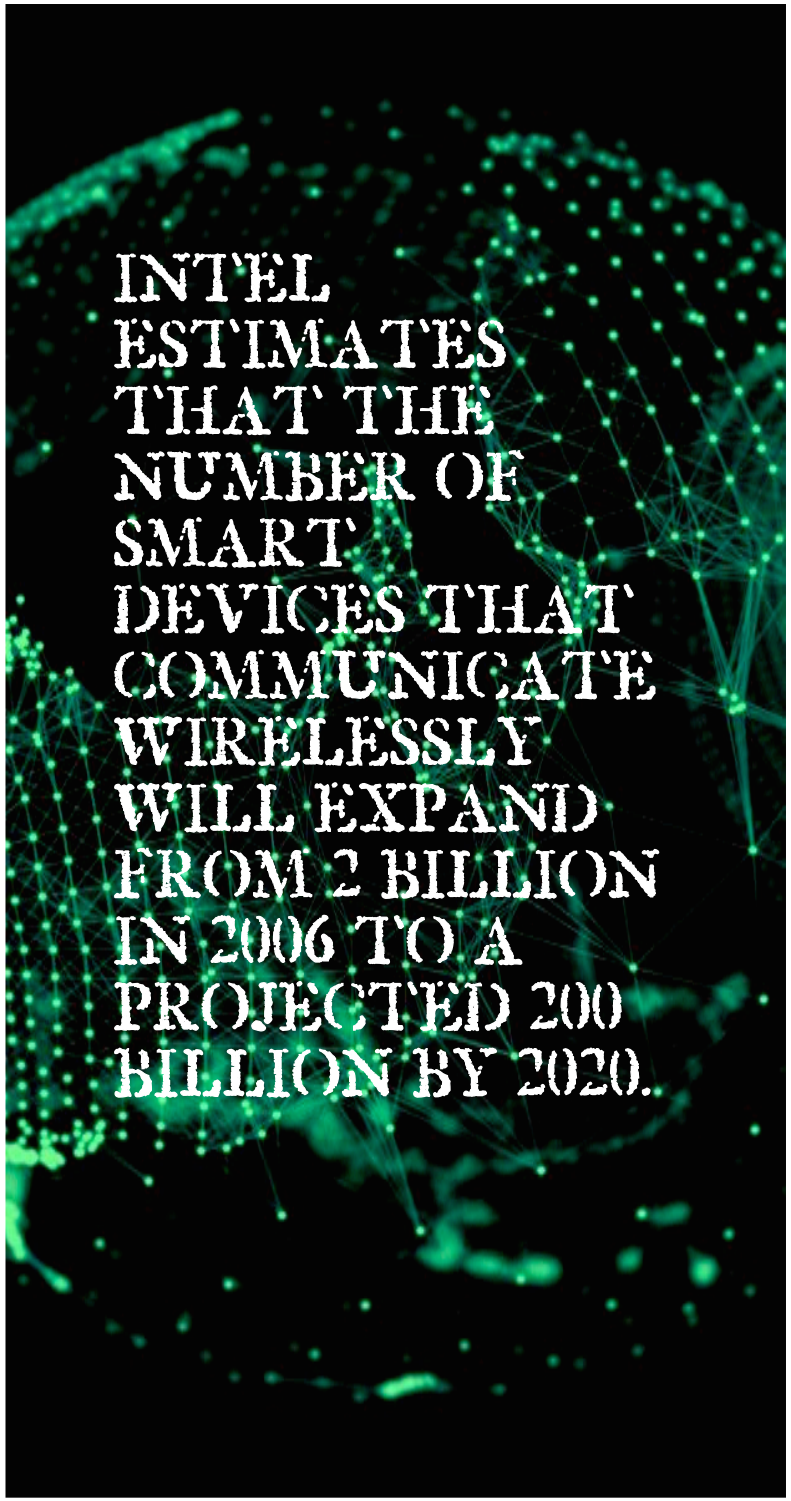
Digitization is underpinning much of the world today – we live in digital times. It's a powerful economic and societal force shaping how we do business, consume, get information, learn, & communicate. It reaches every aspect of most of our lives, from the casual to how we account for ownership and how business is done on a global scale. It has no doubt improved lives and futures around the world. Digitization is fuelling world economic growth and providing a framework for how to rationalize how many things are done, improving on old business models and facilitating completely new ones. The numbers are staggering:

In 2010, Eric Schmidt of Google stated; **"Every two days now we create as much information as we did from the dawn of civilization up until 2003."** Combining Schmidt's estimates with the rate of data growth from 2010 to 2015, ARK Invest analysts' estimates that those two days have shrunk to a matter of hours. Microsoft estimates that by 2020, online data volumes will be 50 times greater than they were in 2016.

Intel estimates that the number of smart devices that communicate wirelessly will expand from 2 billion in 2006 to a projected 200 billion by 2020. As of June 2017, 51% of the world's population had internet access. Cybersecurity Ventures estimates that number will be 90% by 2030.

According to studies by Ocean Tomo, a global corporate risk management consultant & merchant bank, the market value of businesses included in the S&P 500 have gone from having 17% of their value derived from intangible assets in 1975 to having 84% of their value derived from intangible assets – such as Intellectual Property (IP), proprietary data & business systems – all of which are kept largely in digital format. According to their survey series, every industry is now part of the intangible economy. Even property-intensive sectors such as real estate and oil & gas have high levels of intangible assets. So do labor-intensive sectors such as construction and retail trade. Already business investment in intangible assets is now greater than tangible assets, such as buildings and equipment.

Many of these crucial assets are stored and operated in the 'cloud' – most with the various public cloud service providers - which in 2018 had annual revenues of $260 billion in 2017, according to a study by Gartner, the same study forecasts that by 2020 that number will increase to over $400 billion.

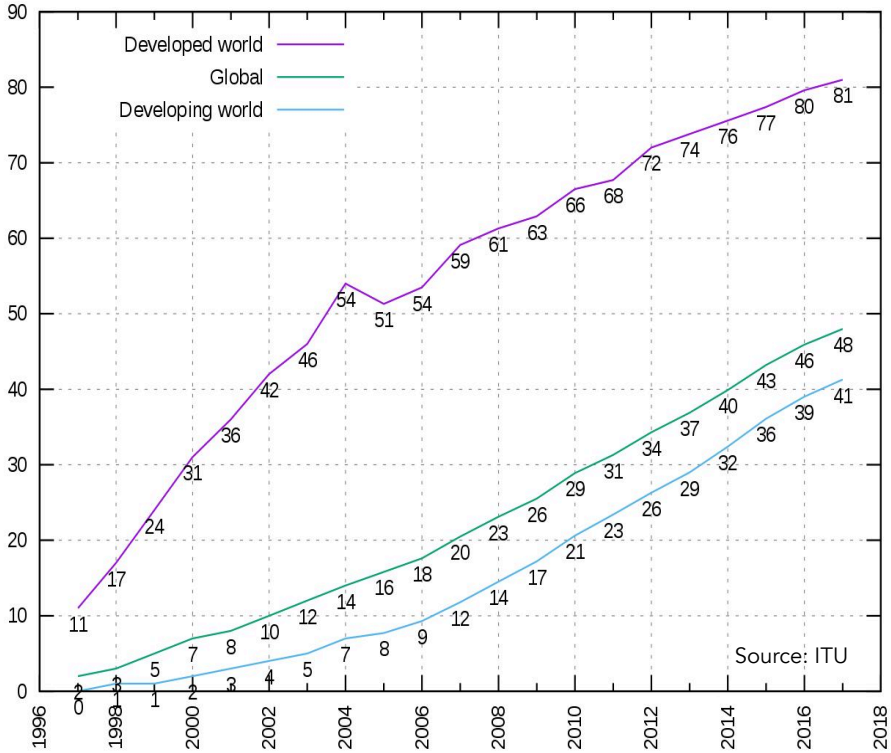


84%

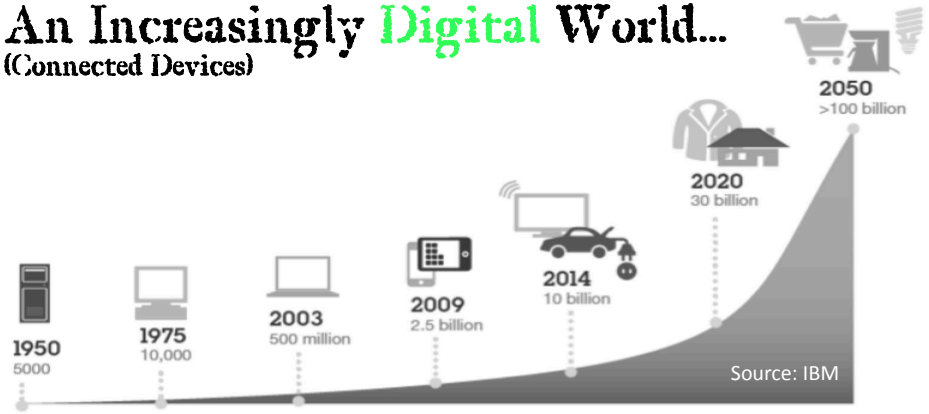
Of S&P500 companies' value was derived from digitally held intangible assets, such as IP, proprietary data & business system, in 2015 vs. 17% in 1975.

Source: Ocean Tomo LLC

Internet Users Per 100 Inhabitants...



An Increasingly Digital World...
(Connected Devices)



"Online data volumes will be 50 times greater in 2020 than they were in 2016"

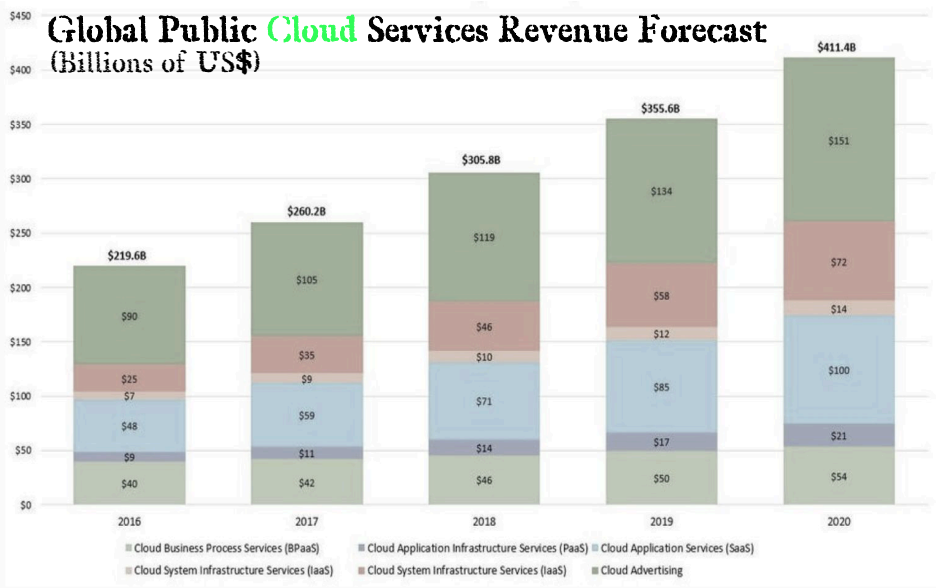
– Microsoft study.

46%

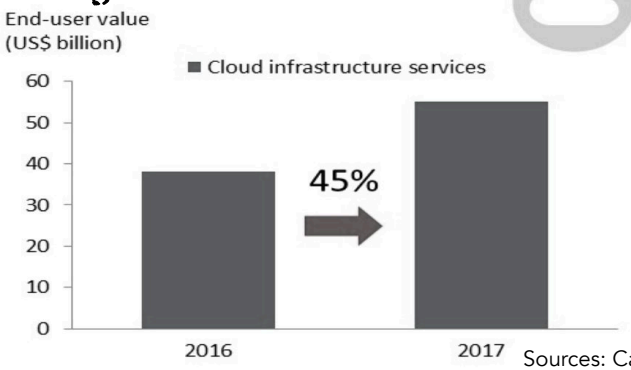
How much the global cloud infrastructure market grew YoY during Q4 2017.

Source: Canalys

Global Public Cloud Services Revenue Forecast
(Billions of US$)



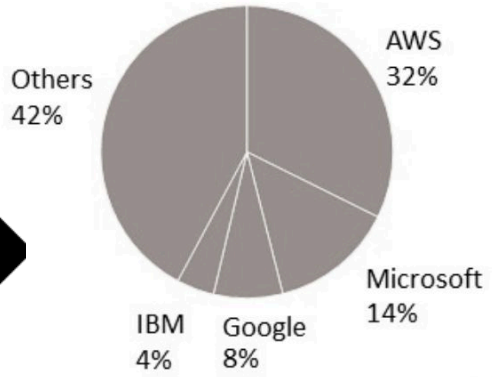
In a digital world, value does grow into the clouds...



Sources: Canalys & Gartner.

Who runs the cloud world?

Q4 2017 market share



A global system powered by digital flows of data...

The World's financial markets went through a rationalization process in the last 20 years moving it to an increasingly digital reality, most financial transactions are done via electronic means today and 100s of Trillion of USD worth of assets are held and traded mainly in electronic format today. The IMF estimates that on average $5.1 trillion moves everyday within the global economy.

FinTech is pushing into all aspects of our financial lives with online banking & brokerages starting to feel like relics and offering such as 'digital wallets' starting to disrupt the traditional 'consumer bank branch' format in developed economies and completely leapfrogging them in emerging markets.

According to Statista; China has approximately 772 million internet users and India has around 332 million most of which are mobile and many use solely payment apps for their financial needs.

Just around the corner is the next step towards full digitalization of financial markets and much of our public & business lives with innovations in public and private Distributed Ledger Technology (DLT) AKA the Blockchain, which could be set to erase the last vestiges to tangible ownership & recordkeeping.

While all this is great and part of mankind's never ending evolution towards better efficiencies and solutions to our challenges, there are a largely unspoken question that has been raising it's ugly head on a number of occasions as of late; **Has the path of progress towards a digital reality outpaced our ability to keep it all secure?**

We have to recognize that with digitization comes increased risks' for governments, businesses and individuals. If not properly addressed, cyber risks have the potential to constrain and even reverse the forward momentum of digitization, which could adversely impact the world economy, financial markets & the wealth and security of families.

$5.1 TRILLION

What the IMF estimates moves electronically on average within the global economy everyday.

For some answers and granular insights into this question and other related ones we decided to reach out to two experts in the field of cyber security. Here Erik & Eduardo provides us with their thinking on these important matters and helps us establish a framework for how an investor can best approach this new reality – both in terms of protecting their assets and for investing into this fast growing industry.

So, Erik & Eduardo perhaps you can start of by introducing your self and providing our readers with an overview of your backgrounds and current projects?

Erik: Having spend the last 17 years in a wide variety of technology focused roles within the financial industry, from network engineer to CTO, CISO &a stint as trader I have build a broad range of competencies and an understanding of what is important and what is not when it comes to cyber security.

Together with the other members of the team at InCyber we constantly seek to develop solutions that can enable CEO's, entrepreneurs and investors to operate and grow their businesses while knowing they have the support they need to navigate this complex and fast evolving sphere.

We know what works in the real world and what doesn't. What's going to work for a certain business & what is not. So each individual business get's its own proprietary cyber security risk model. With that we can help prioritize the risks and provide the solutions to overcome those challenges in a transparent and flexible manner.

The cyber security industry, much like the financial industry, has developed this whole edifice of a special language with overly complicated terms and crazy words that can seem daunting to the average person, trying to manage their business and while aware of the threats broadly it can be difficult to find the right set of comprehensive solutions.

My mission and the work we do at inCyber Security is all about providing those solutions in a clear and practical manner that enables our clients to make informed decisions and the ability to go about their business knowing they have a solid partner helping them protect their business from this constantly evolving risk, and of course where possible helping them cease the opportunities that this changing landscape has to offer.

Eduardo: With my background in management consulting, where you get to see the granular challenges facing businesses across many industries & work to build systems and processes to turn those challenges into opportunities, I have followed the cyber security space for decades and seen the constant evolution.

I have a broad interest in global financial markets and its infrastructure, which along with my experiences across Asia, Europe and North America has led me to my current path. Where I spend time at MIT in my commitment to life long learning and I have pursued a more hands on entrepreneurial approach and cyber security was both a natural fit and clearly an amazing sector to build a business for the future in.

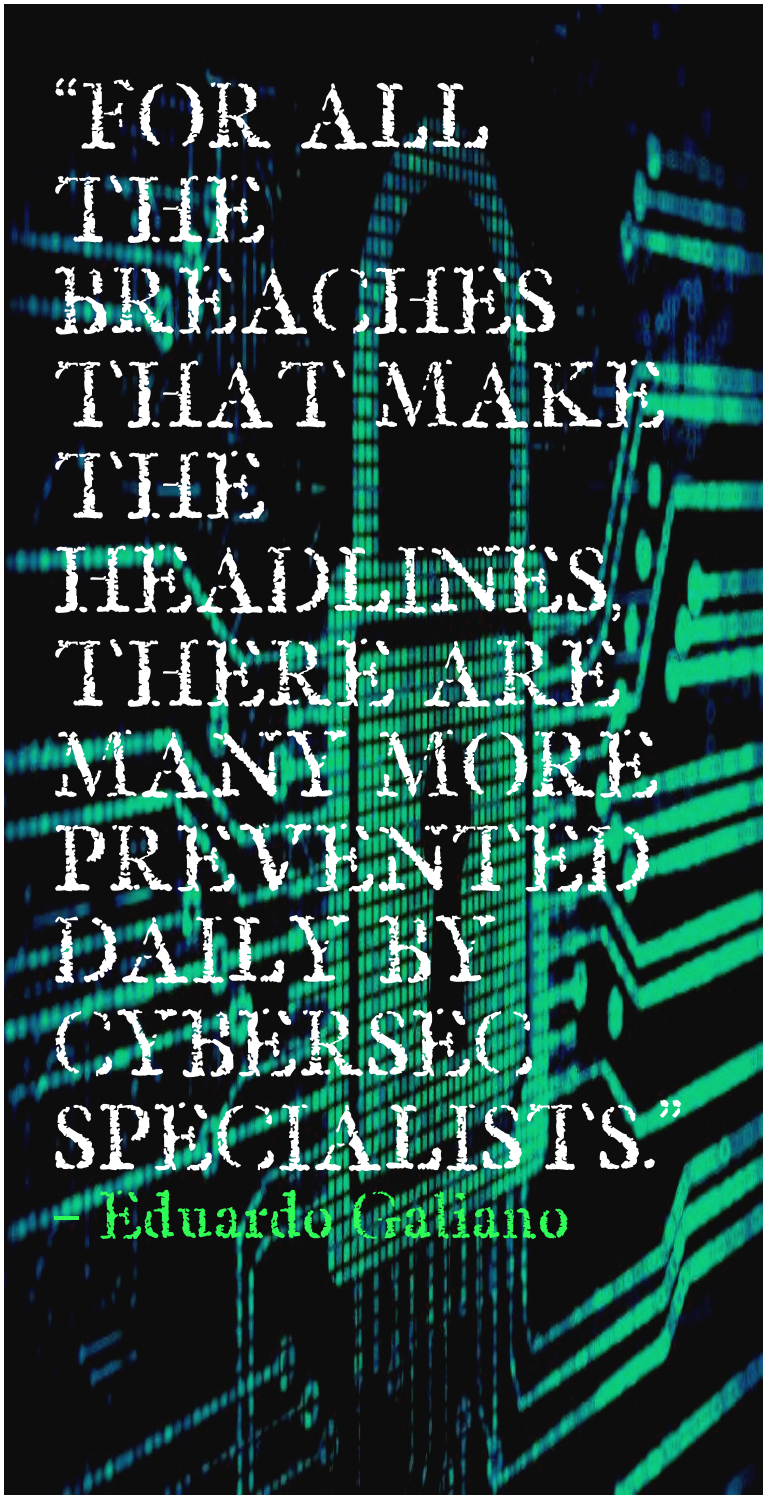
In the last decade cyber security has become a critical mission for national security, and a board level issue. Apart from breaches and incidents seen in the media, there is much more turbulence beneath the surface and it now includes space as a battle domain. It became clear to me over the past 2 years, that the risks were accelerating due to technological sophistication and access to "Hacking as a Service" (HaaS) by criminal groups and nation state backed groups moving between profit, espionage, & geopolitics.

When we look at both our daily and work-related lives, how we interact with technology, databases, IoT, even the web-connected cars we drive, everything touches the internet, everything has a connected IP & port address. Add the linkages to vital infrastructure we all use and suddenly, genuine cyber risk is everywhere.

70% of senior executives have made cyber security decisions that affect policies and security but yet no major business school teaches cyber security as a major field of study. Across the spectrum in fields from healthcare to manufacturing, cyber security is left to the IT professionals or Chief Information Security Officers (CISOs) especially in the larger organizations.

For all the breaches that make the headlines, there are many more prevented daily by CyberSec specialists & their staffs. It's not uncommon to hear from them "we are pinged all the time especially during peak hours of consumer operation." The majority of organizations do not have these kinds of resources. Never mind private individuals, ask yourself; how much you've thought of or even formulated a plan in case of personal breach/attack/ransom ware? How prepared are you?

Along with Erik we are working on offering automated solutions that helps policy makers, business leaders and individuals plan and manage their digital reality with a comprehensive cyber risk management approach.



Q: So going back to our synopsis and core question; Has the path of progress towards a digital reality outpaced our ability to keep it secure?

Eduardo: The path stretches back from old to new, from the most advanced personal area, the Internet of Things (IoT), to the oldest, Industrial Control Systems (ICS), and across personal devices technology has moved ahead exponentially but not all security practices and legacy systems have kept pace with the digital threats.

IoT might just be the weakest link in our modern lifestyle. Smart home appliances from refrigerators, smart TVs & camera monitors are inside our most personal networks, right next to what could be your private conversations or sensitive data stored on thumb drive sitting inside an unpatched home pc. Some are managed by 3rd party providers, which brings the following questions to the forefront; how often are they patched? Have they been adequately segregated from the network? Have you upgraded the firmware on an older wireless printer? Vulnerabilities exist that exploit these exposed points to access data to insert malicious files etc.

Our personal smart phones are fairly secure IF all the right features are utilized such as 2FA and password managers. But they're susceptible to social engineering tactics that can compromise one's identity leading to further penetration.

Erik: Social engineering is a hot topic, it's a 'man in the middle" intrusion techniques. Standard confidence plays like calling on the phone requesting passwords impersonating IT department or simply walking into an office dressed well and sounding like you belong, in order to access a workstation. This is where the area of human interaction offers innumerable entry points to get at private data, passwords, and location.

I personally think the science of human factors may come in to play going forward. Essentially, training those in the circle of trust to be diligent, aware, not afraid to call out something unusual, irrespective of department or status, will play an important role. A human team effort to go along with digital security systems including AI, but the larger the institution the more gaps will inherently develop and increasingly savvy actors will pinpoint such weaknesses and seek to exploit them.

You can be doing all the right things 99 times out of 100, but all it takes for the other side to gain entry is that one time they penetrate the system. Awareness and constant evolution is key.

Can you give us some examples of the risks facing global businesses today, perhaps with some actual examples of situations that have taken place in the last couple of years?

Eduardo: While IoT gets a lot of attention, as people speculate about the risks of the future, the past is still with us and holds a lot of largely unaddressed vulnerabilities that are both broad and that demands attention to avoid potential major interruptions to societies & the global economy. Industrial Control Systems (ICS) has been with us since the 1960s in various formats and some of our crucial infrastructure, both public and private, still runs on stable but rudimentary systems designed in a different era.

Looking deeper into the realm of ICS, the outlook appears very disconcerting. This segment encompasses the entire spectrum of modern life. The power grid, water and electrical utilities, gas power lines, manufacturing, and everything that is networked around it; even the smart meters on the side of your home are part of the system. Here you have 1960s-1980s Supervisory Control and Data Acquisition (SCADA) systems that is, in many instances, open and exposed.

In many instances these systems are running outdated or hardcoded software without up-to-date patches or security silos to prevent access. These control and communication systems are 'core mission' processes that can ill afford down time outside of regular maintenance/update cycles. Hackers rarely show such courtesy when they decide to strike.

It seems illogical at first but one should realize these gas pipelines, power transmission lines, and water plants were on their own digital systems, isolated from the business (HQ) networks. With the advent of Windows and ethernet networking systems in the 1990s, owners of these systems expected connectivity and monitoring for greater transparency and productivity. All fine but the systems were not designed to be updated beyond scheduled upgrade cycles.

ICS is not IT, that is to say, these functioning legacy systems were not designed with modern cyber security protocols in mind. This convergence of IT & operation technology (OT) require two disparate disciplines and are not designed to overlap. We could go further with a look at similar issues with UNIX servers and Wi-Fi networks, but it's important to understand a critical system that was designed to operate in a fault tolerant manner is not the sort of system that can be patched, rebooted, or scanned with normal security software.

What can be done? There are techniques & best practices that address, but not eliminate, these security risks but they require multi-disciplinary teams working together to ameliorate the risks. It's a challenge as the logic programmed into the precursor PLC designs did not factor in how to incorporate modern security scanning and penetration testing.

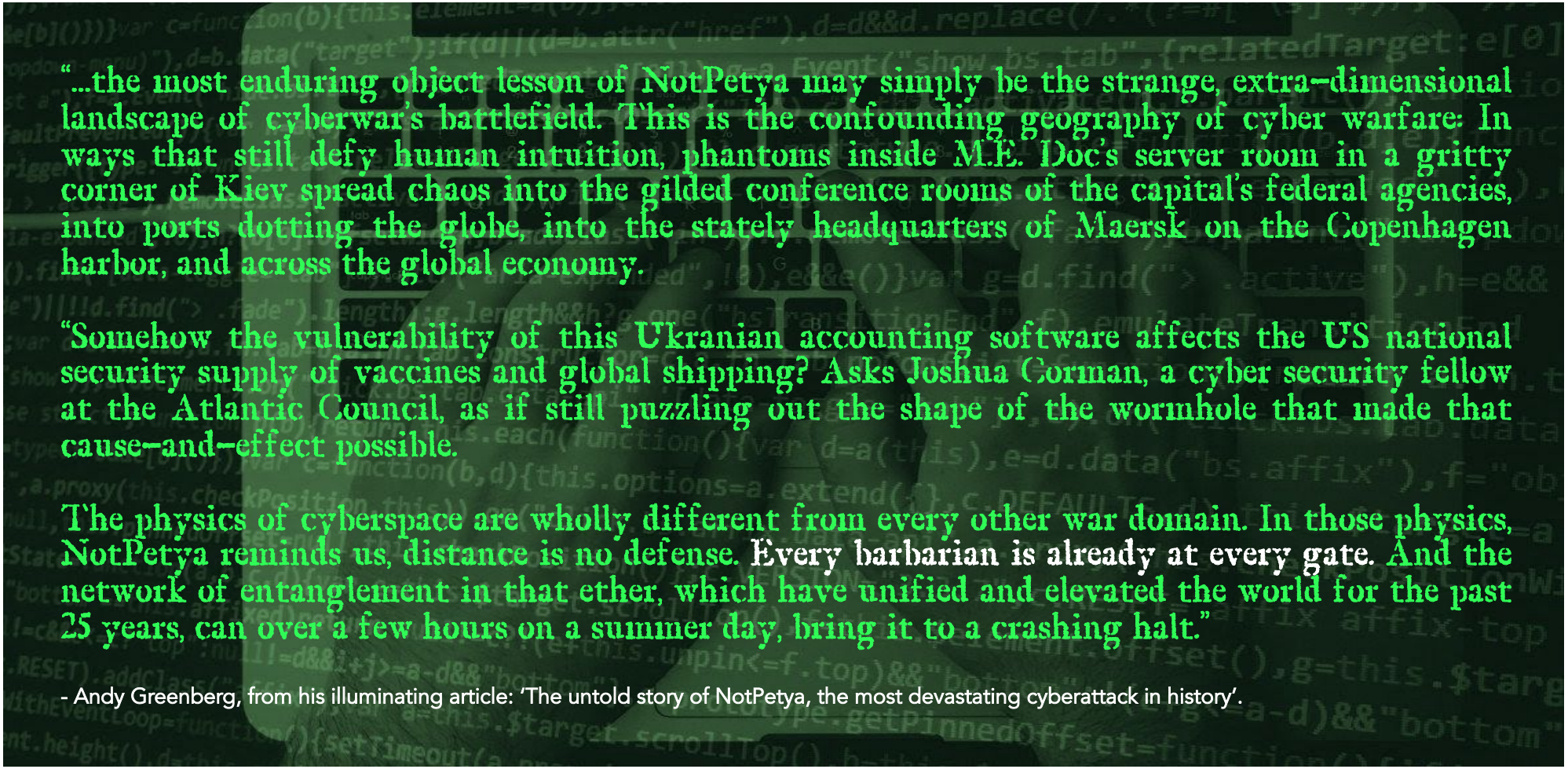
In essence the whole infrastructure will need to be replaced with smarter solutions at some stage which will be costly but it will provide opportunities to develop solutions for the future that could become competitive advantages. We are starting to see some of this with the development of so-called 'Smart-Grids' for example.

Military leaders are well aware of this, in the US it's estimated that over 70% of the energy needs for the DoD is dependent on such systems.

Of course we don't advocate hacking but to get an idea of what's available to ANYONE, you now have online scanning tools, www.shodan.io is one, where ANYONE can scan the WORLD looking for EXPOSED IP addresses and unprotected ports. ICS systems show up repeatedly and have already been targeted on several occasions.

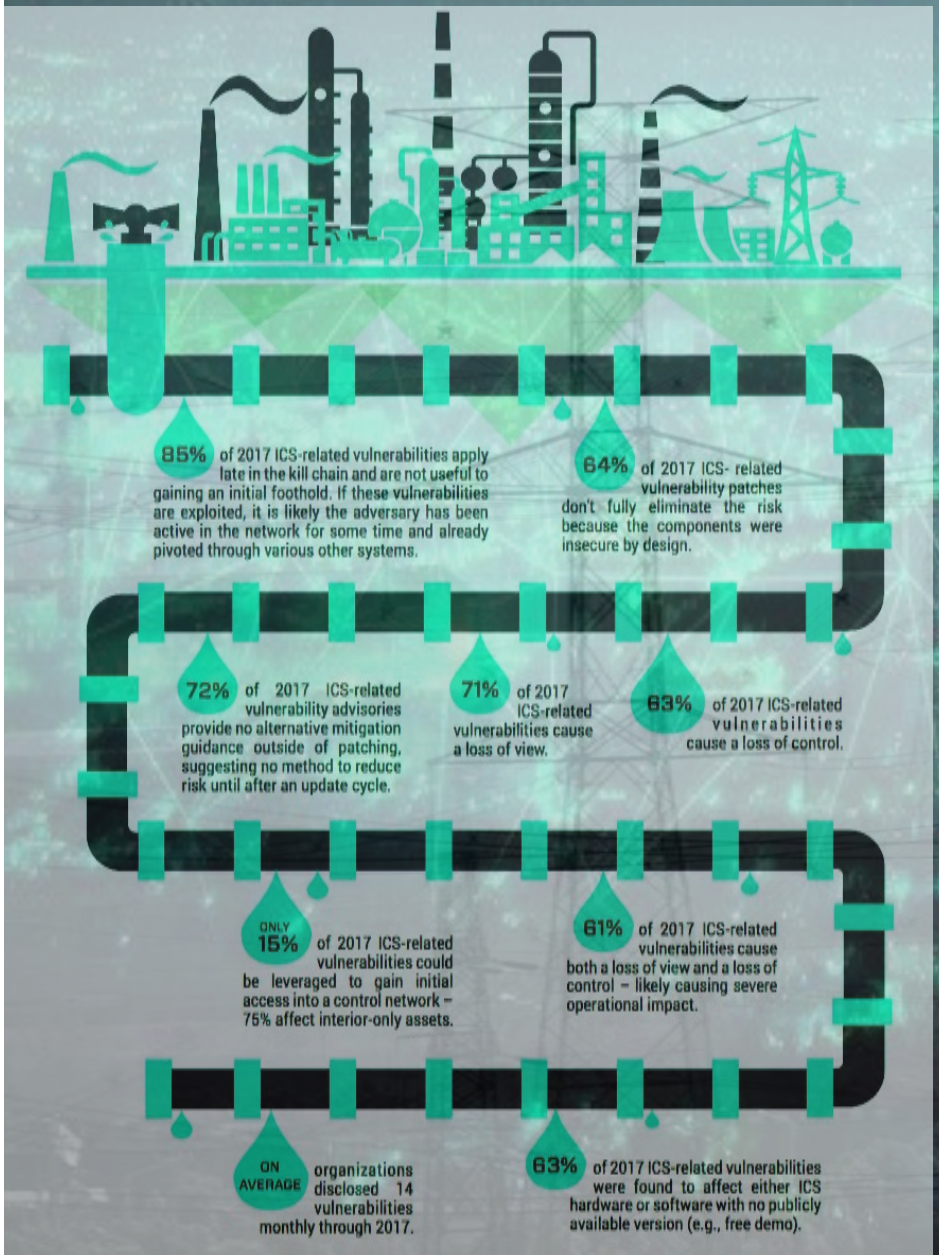
You're not just up against hackers but nations states potentially attacking ICS in the event of cyber warfare or colluding to go after large wealth, such as the theft of $81m from the Bangladesh Central Bank through the SWIFT system.

We could even see alternative power grid providers set up in regions isolated from main population centers etc. as a way to combat this threat. It's pretty dystopian but the threat is all too real.



The vulnerability of our ageing Industrial Control Systems (ICS) is an inconvenient truth and an opportunity...

ICS VULNERABILITY FINDINGS 2017:



Source: Dragos Inc.

Q: The targeting of governments and national interests has received a lot of focus after the 2016 US elections, Russian cyber attacks on Ukraine & more recently with the rising awareness of China's efforts in the space. How do you view this space & what are the likely paths ahead here?

Eduardo: The area of state-sponsored actors is now better understood by DefSec pros & cyber security specialists in addition to greater media awareness. What is not well understood, except by bad guys & nation state actors is just how open our digital systems are and how fragile our way of life is to various cyber threats. From increased use of ransom ware and hacks to theft of IP sitting on one's pc, smart phone, or thumb drive.

Large corporations are generally doing a good job but it's still hit or miss as breaches keep occurring. Greater risk awareness and adherence to robust data security and privacy standards are needed – and it's coming with GDPR etc.

In regards to China, there are armies of hackers working on penetration testing and reconnaissance for IP theft or malicious intent. This is undeclared asymmetric warfare. There is no power on earth that can stand up to the U.S. military, so to level the playing field, one goes where one can create that asymmetric advantage. In this case, our open society and democratic norms of trust and open exchange with data are vulnerable by design.

A key challenge here is attribution, how can you prove that that the malware or device came from X country? There are indications for example if attacks and data logs show activity from 8-6pm Asia time, but attribution is problematic for private entities.

In this regard, an evolving paradigm we are seeing is the private sector & law enforcement, particularly the FBI, in cooperation and coordination before a breach, IP theft or ransom ware occurs. There are government cyber specialists who liaise with private & public companies to prepare and/or address breaches. This new paradigm is interesting, many people may not like it but the threat actors are well funded & highly skilled that it maybe be better to have expert help with the recourses of government on one's side.


There are two types of companies: Those that have been hacked and those that will be...
Hacking as a Service (HaaS):
Ever since the first reported cybercrime in 1973, when Union Dime Savings Bank account data was manipulated, cybercrime has continually evolved. Beyond a nefarious hobby, cybercrime has become a way for cybercriminals to earn a living. While it remains underground, it is a business nonetheless; attackers cooperate, and work to maximize profits and minimize risk of arrest. Cybercrime as a profession is increasingly attractive for able hackers, and in turn, cyber attacks themselves are increasingly well organized. With the wide-spread adoption of the "Haas" model for cyber attacks, the attacker can purchase the desired "service" through the dark web without so much as a cursory understanding of what is involved in its execution.
HaaS Fees 2018:
• Hacking a Facebook or Twitter account: $130.
• Hacking a Gmail account: $162.
• Hacking a corporate mailbox: $500.
• Scans of legitimate passports: $5 each.
• Windows rootkit (installing malicious drivers): $292.
• Winlocker ransomeware: $10–$20.
• Unintelligent exploit bundle: $25.
• Intelligent exploit bundle: $10–3,000.
• Traffic: $7–15 per 1,000 visitors for the most valuable traffic (US & EU).
Source: MIT

Q: Can you talk a bit about the kind of threats business people, government officials and investors face when traveling to high risk regions from a cyber security perspective and perhaps suggest some ‘best practices’ for our readers to consider?

Eduardo: There was a recent case study done by Recorded Future focusing on a few cases of what appears to have become standard operating procedures from China. According to the study In May 2018 the office of Alaska State Governor, Bill Walker, announced a trade delegation titled "Opportunity Alaska" to visit China. After concluding the mission, led by Gov. Walker, media reported disappointing prospects for several 800-mile gas pipeline projects. The President of China's largest refiner, Sinopec, was quoted saying, "I think there’s a lot more work for us to be done than originally imagined.”

Between April 6 and June 24, 2018, Cyber security firm Recorded Future documented over one million IP connections between Tsinghua University [China's elite Tech University] and networks belonging to the State of Alaska Government and private entities including: The Alaska Communications Systems Group, Alaska Department of Natural Resources, Alaska Power & Telephone Company, and TelAlaska.

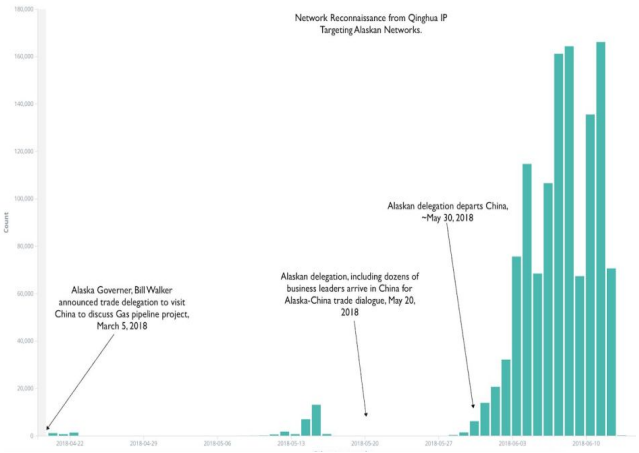
"Scanning activity against Alaskan networks in late March, only a few weeks after Gov. Walker announced a trade delegation to China. The activity picked up for a few days prior to the delegation arriving on May 20, 2018, and dropped off as the delegation arrived. Probing of the Alaskan networks remained at low levels until May 28 as the delegation concluded its activities, then ramped up considerably as delegates left China." On June 19, Gov. Walker announced a trip to Washington D.C. to "discuss trade tensions with U.S. and Chinese officials."

Recorded Future noted, "a further surge in [network] interest between June 20 and June 24 against the State of Alaska and Alaska Department of Natural Resources networks." Tsinghua University, like all institutions, is assigned a unique IP domain that allows researchers to trace outbound activity and analyze host-target log records. The bulk scanning of ports is conducted to find network/hardware vulnerabilities in order to gain access (via a backdoor).

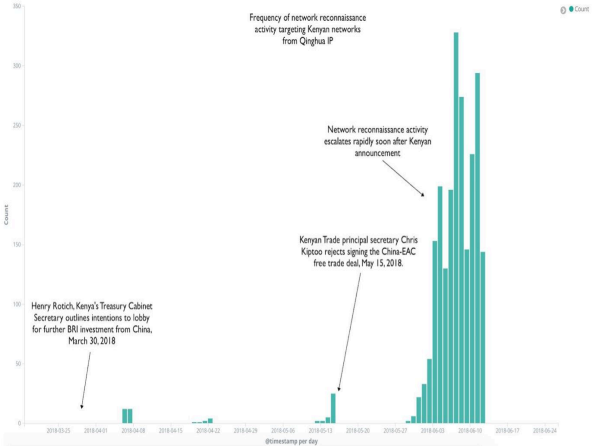
Similar network reconnaissance emanating from the Tsinghua IP have also been documented against the United Nations' office in Nairobi, the Kenya Ports Authority, Brazilian organizations, Daimler Benz, etc. It can be surmised that cyber espionage is being undertaken in support of China's policy directives (energy, trade, geopolitical - 'Belt and Road Initiative').

Government and private organizations should expect these scans and intrusions to be undertaken against them, particularly around high-profile negotiations or announcements dates. Cyber security countermeasures must be implemented and vulnerable access points secured before any headline news events.

Network probing events by Tsinghua IP targeting Alaskan institutions coinciding with Alaskan trade delegation to China in May 2018.



Network recon events conducted by Tsinghua IP targeting Kenyan institutions overlayed with key China–Kenya economic developments.



Source: Recorded Future

BEST PRACTICES FOR BUSINESS TRAVELERS:

Eduardo: As for best practices for business people, government representatives and investors when traveling, every case will be different depending on your role and the place you visit etc. but here are a few useful ideas;

SECURE YOUR DEVICES – Firstly if traveling to high risk areas consider what devices you actually need to bring and in some cases companies provide so-called 'burner' mobile devices and laptops for complete separation from daily data. Secondly lock your devices using security settings for PIN number and fingerprint ID, ideally in a two step format including both. Change your PIN regularly and especially if your device has been temporarily misplaced or left in your hotel room.

ACCESSING THE INTERNET - Avoid public Wi-Fi and if needed avoid accessing personal accounts or sensitive data while connected to the network. Most devices have a setting that allows it to automatically connect to any Wi-Fi networks as you pass through them on your travels. Before travel you should change this feature so that you must manually chose to connect each time you wish to access the internet. Use commercial VPN services for all connections. The same precautions goes for Bluetooth connectivity which just like automatic Wi-Fi connectivity can provide hackers with an easy point of access to your devices.

MINIMIZE LOCATION TRACKING – Avoid sharing your locations via social networks or by posting photos while traveling in high risk areas. By sharing too much information publically you make it easy to track you and identify your daily routines. Limit the information you post online about your specific whereabouts to limit threats to your personal property.

BUILD A SHIELD AROUND YOUR DEVICES – Ensure you have up-to-date Anti-Virus Protection installed with automated alert services. Use PIN codes of high complexity for all aspects including password creation for hotel room safes & gym lockers.

BETTER SAFE THAN SORRY – If you suspect that your devices may have been breached, immediately alert your business administrators, banks and other custodial service providers and have all aspects checked and monitored for unusual activity and have new security features re-issued.

As mentioned, every case is different but if you are a high profile individual you will be targeted, so make sure you have a comprehensive set of solutions implemented. We at www.incybersecurity.com can help you with this, so please feel free to reach out for a conversation on this important subject.

Q: From an investor's perspective, in terms of protecting your digital assets, what are some of the risks to be aware of and what are some of the tools you would consider as a key to negating such risks?

Erik: We can separate "best practice" into two buckets. One for organizations and the other for private individuals. For the former there exist very comprehensive compliance & regulatory standards that help mitigate risks and lawsuits. The frameworks are of course technical; they include National Infrastructure Protection (DHS), National Institute of Standards & Technology (NIST), HIPAA (Healthcare) ,and ISO among others. The landscape is becoming better regulated with growing data/privacy protection laws. The EU's General Data Protection Regulation (GDPR) followed by California's new data privacy law which mandate how private data is managed show the trend here. It also offers opportunities for investment.

With the advent of **crypto currencies** as an asset class, we now have digital wealth to protect. The name of the game is the data, finding it, stealing it, using it, hiding it, erasing it, or even manipulating it.

What works to protect this data:

- 2 Factor authenticate EVERYTHING.
- Use commercial VPN service for connecting in public Wi-Fi areas and when overseas.
- Utilize endpoint protection (standard level of security across personal devices, networks, and wireless connections).
- Central logging and analytics offered by various software vendors.
- Cloud backup (in case of ransom ware or physical loss).
- Education & training, "how to maintain a secure environment."
- Behavior management changes regarding phishing/social engineering.
- Consider using "burner-devices" (laptop/phone) for travel to high risk areas.
- Try to use encryption technologies whenever possible.
- Concerted effort to patch & update your own devices & hardware (software tools available).

Consider using a Silo Browser that runs in the cloud giving you a secure way to access the internet. The advantage is that your device is completely isolated from the web exploits, nor are you receiving any codes. https://info.authentic8.com/secure-browser

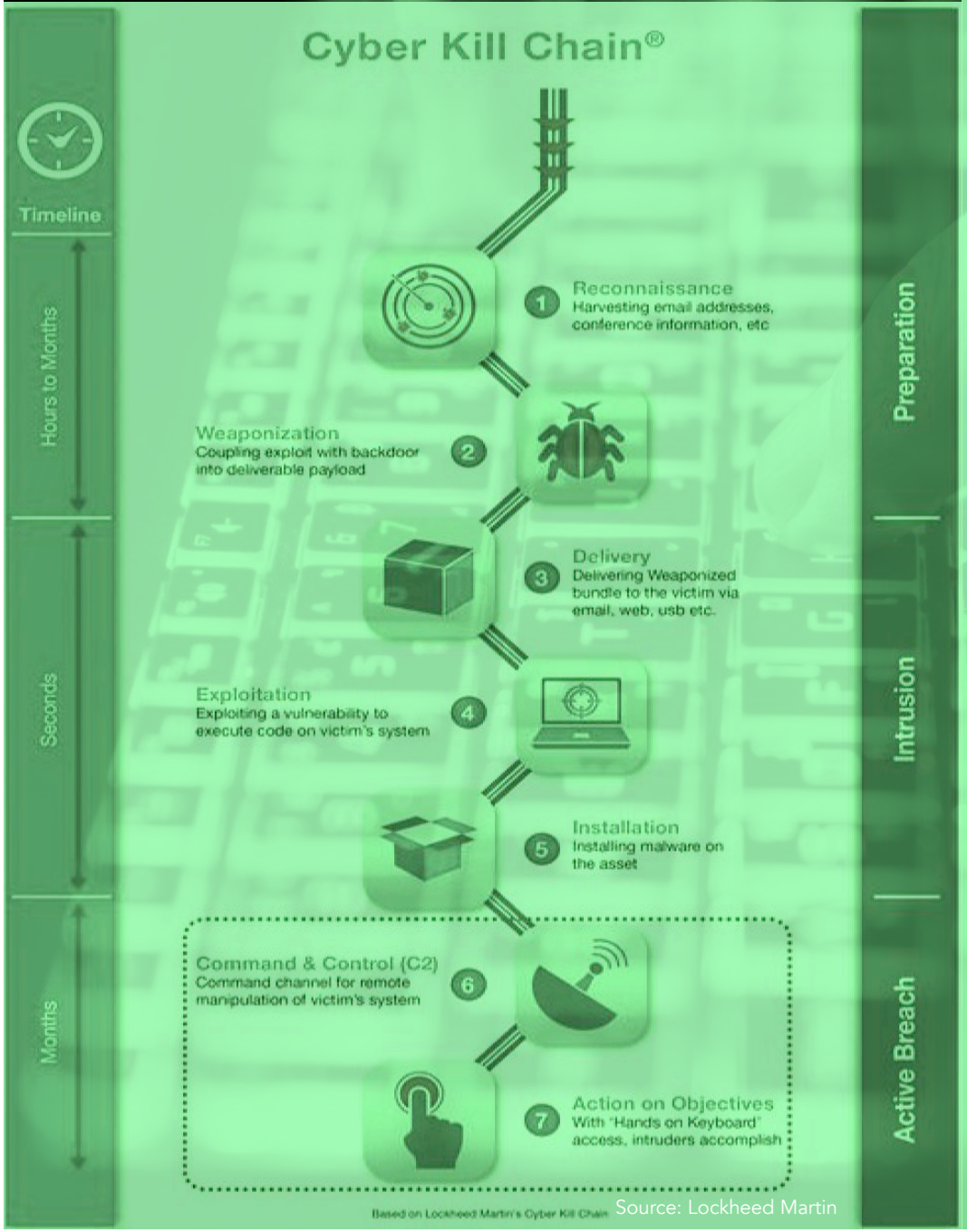
Lastly, assume you have been breached & a hacker is scanning and looking for an opportunity to hit & extract data. What are your personal policies and procedures in such an event? Have you found experienced legal council to go over a well-thought out & worded cyber security policy.

A Case Study: A HNWI is targeted via his broker/custodian using simple tools.

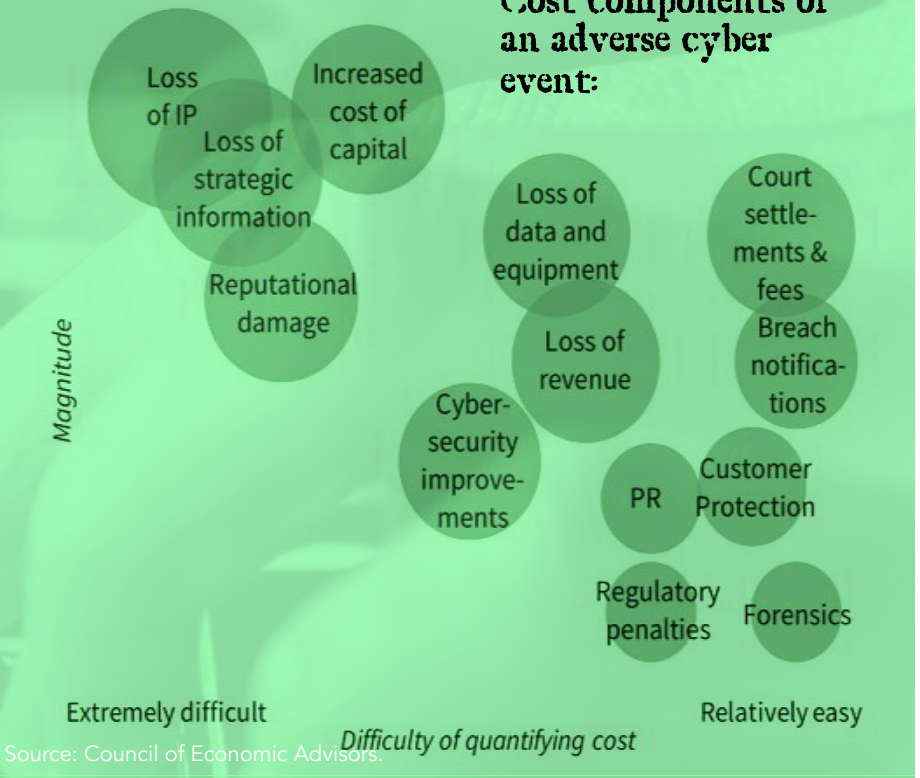
An employee's company mail, working for the broker/custodian, is breached. Private info such as account numbers, balances, wire info is read. Hacker then sends hi-jacked mail to all clients on compromised employee's list. Client receives dummy but similar looking mail with a malicious PDF link to forward and check login credentials. Client assumes normal and goes ahead to login to a "dummy" but similar looking website. At that point, hacker has all he needs to send out wire request of X amounts of millions. Not an unusual request for an account of the size of a HNWI client & in line with the nature of a trading account.

The vector used to initial transfer out from brokerage firm was the DATA inside a compromised internal email. Note that no real technological sophistication was needed or required after the compromise. All the tools needed could easily have been "off the shelf" (HaaS). Fortunately, the firm had callback procedures in place so that once the client was called, they denied initiating the transfer. Social engineering works because of the natural willingness of people to help and the human trust element when they believe they are dealing with someone inside an organization.

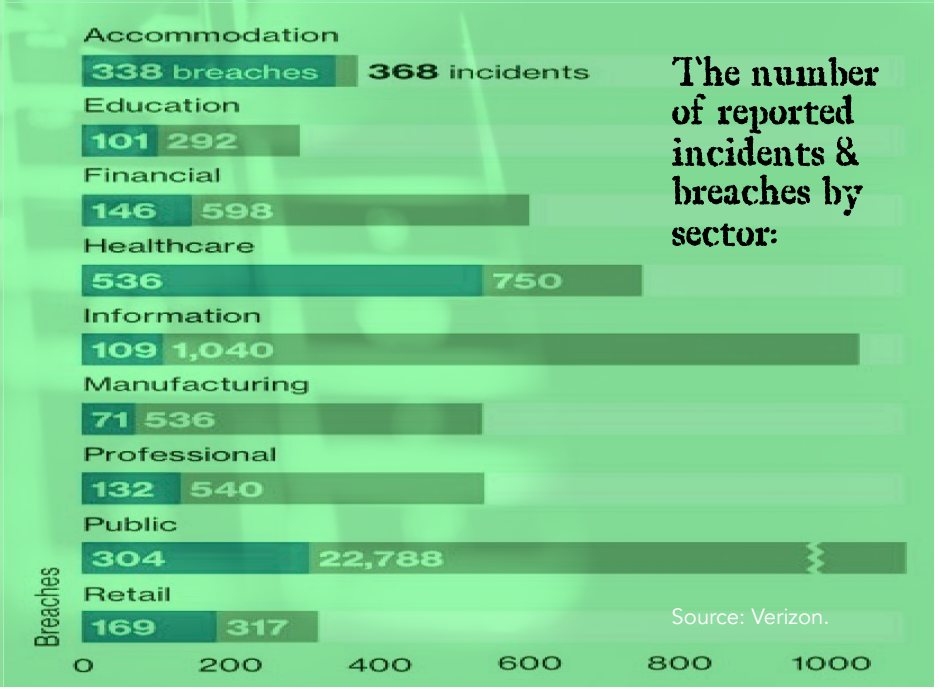
INSIDE THE CYBER KILL CHAIN...



Source: Lockheed Martin



Source: Council of Economic Advisors.

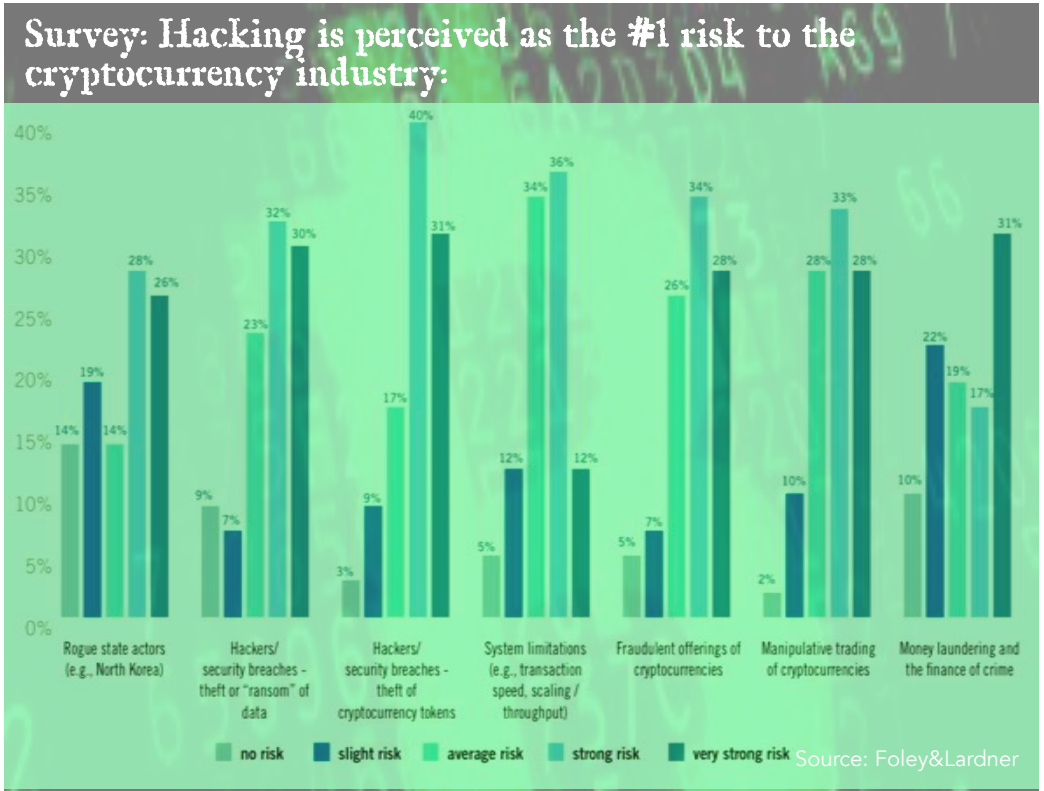


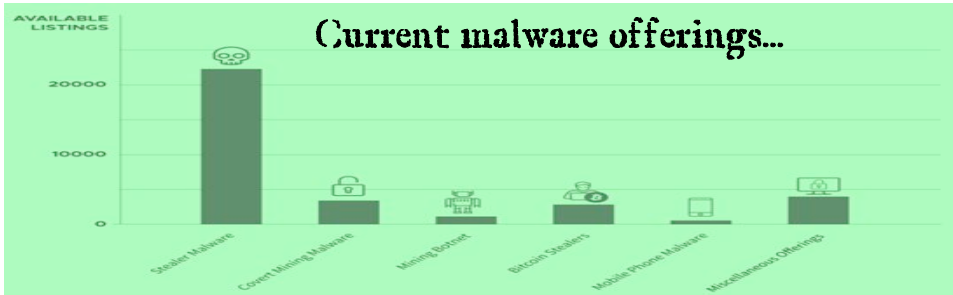
Source: Verizon.

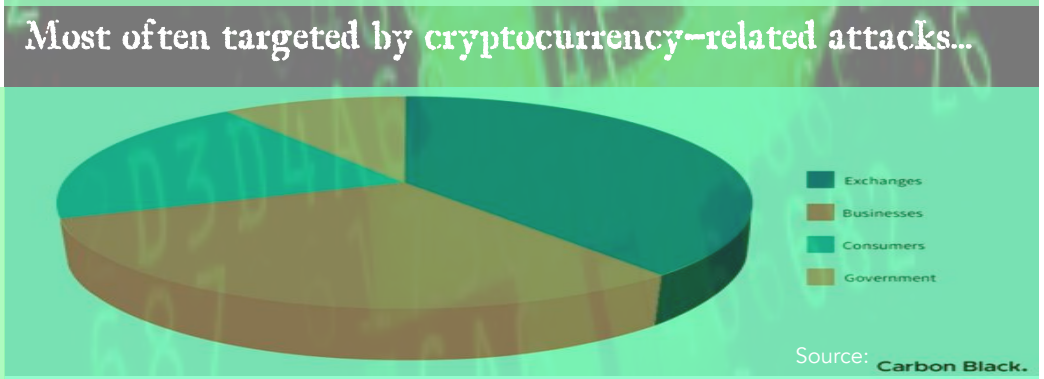
Q: For our readers who are interested in the crypto space – digital currencies & tokens – what are some of the risks there to consider and what can you recommend in terms of securing your holdings from some of the known risks?

Erik: The risks are straightforward – here are some general advice that everyone should adhere to. For larger players such as institutional investors and asset managers you should have a tailor made set of solutions in place, we at inCyber do a lot of work in this sphere and can help you build a secure and optimal system for your operations.

1. Theft via hacking (Note recent amounts stolen from crypto exchanges).
2. Private key management, i.e. NEVER keep them inside an email address nor save them in plain text doc on your pc or device.
3. Consider securing digital assets that reflect investment goals, are you a "Hodlr", or speculator, or business. The nature of the answer will dictate just how much security to add.
4. Consider leaving it offline in cold storage; Online ALWAYS has higher risk.
5. Do not leave assets at the digital exchanges where most breaches occur.
6. When transferring always use encryption, avoid public WIFI (Airport's are the biggest "NO").
7. Be aware who's physically around when digitally moving account data.
8. Whenever using any 3rd party vendor, ask what are their standard security practices? It should make sense and be to a high standard (NIST). If it doesn't sound good, then always call a professional's like us at www.incybersecurity.com.







Many Bitcoin investors/enthusiasts often bring up the security factor related to the DST/ Blockchain as an effective tool for securing records of transactions and holdings – how do you see this?

Erik: Definitely, that's what it does better than any other current solution. The current weaknesses in the system lies at the points of interconnection between the Blockchain/DST solutions and the outside systems such as the exchanges and "wallets."

Do you think the technology has potential as a security feature for other areas?

Erik: Not entirely sure yet, time will tell. There are new services being developed, but they have not yet been "stress tested" sufficiently to make a measured assessment. But lot's of very clever people are working in the space and innovation will no doubt bring some great solutions to challenges across different industries.

In other areas, like asset management & custodial services, the immutable feature of Blockchain and the hash feature, to Identify changes, does overlay a sense of structure that can't be altered.

You could even consider attaching Blockchain tech to a website to prevent hacking, one would expect to see X but instead sees X+2 etc. Any changes to data could not happen without proper authentication in place.

In the private DST space and in the application of 'Smart Contracts' there are real big players such as central banks and big global exchanges like ICE who are working on improving their systems with the technology. Recently we noted that China's Supreme Court stated it "recognizes Blockchain evidence as legally binding." It is certainly a space to watch both in FinTech and other sectors.

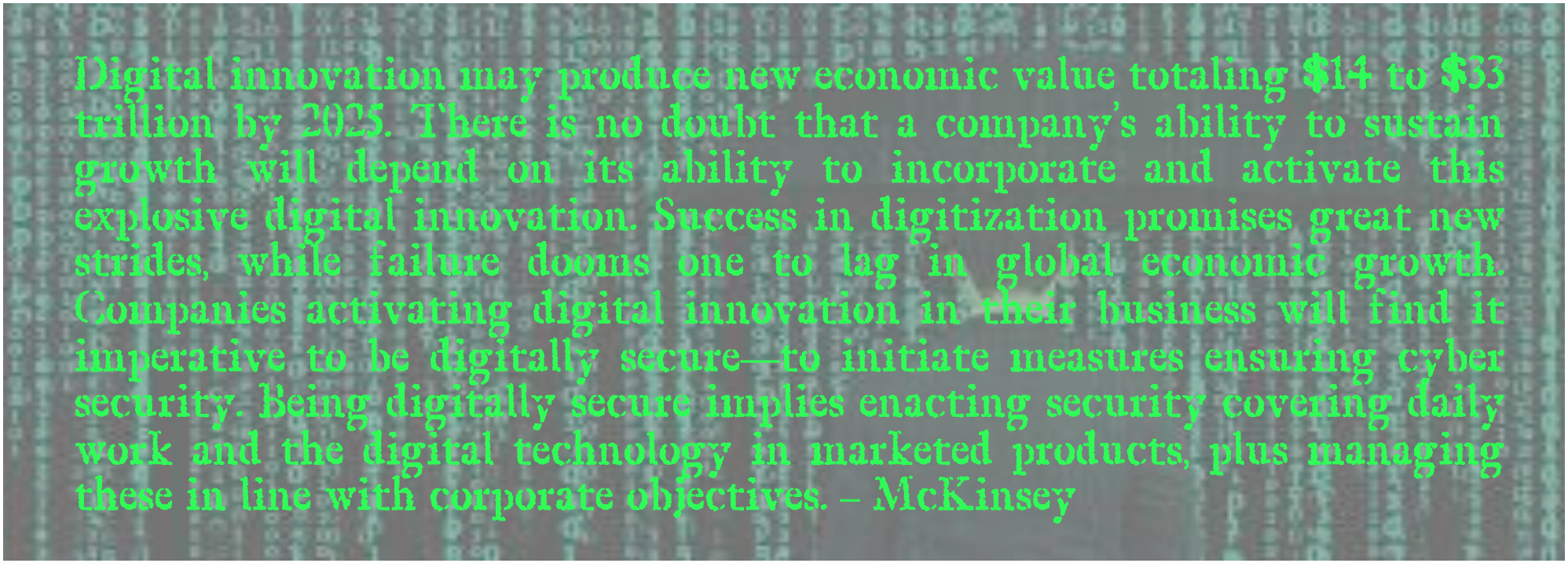
Q: What are some of the most interesting areas in the crypto/digital assets/FinTech areas from your perspectives?

Erik: Number one is the use of software, like our own Cyberdash, to automate regulatory compliance across a firm's endpoints, that includes cyber insurance. Barclay's estimates that market to grow to $20bn by 2025 from around $2bln in 2017 (See the 'Investment Opportunities' segment at the end for a look at the Librarium teams views on this interesting space).

The software and IT solutions that address GDPR type standards will offer new growth areas. Providers of solutions to meet higher regulatory privacy standards will benefit. Yes, compliance adds cost but with automation it will be much more bearable.

The ability of smart contracts to monetize assets has us very excited. For example, one could track, insure, and trade an entire LNG ship load down to the token level across the entire supply chain. We're hearing of insurers willing to offer risk products down to the token.

With China's Supreme Court evidentiary Blockchain rules, smart contracts will be more widely accepted and used for business or commodity trading purposes. Others will follow.



Looking to the horizon, what do you see as some of the key developments to look out for?

Eduardo & Erik: The most immediate and promising area will be 'cloud migration'. By 2020 85% of large enterprises will be using a Cloud Activity Security Broker (CASB) platform from less then 5% today (Gartner). These new platforms will allow local security controls inside cloud data. This is a big plus as users will be able to apply behavioral analytics and anomaly threat detection algorithms inside cloud applications.

Understandably, having private data off site still makes the majority of people uneasy. But what's the alternative? Being exposed, trying to manage 24/7 every Common Vulnerability Exposure (CVE) published daily, patching aging systems or worrying where exactly a threat is hiding and learning your systems, procedures to go after your digital crown jewels.

Our own area, RegTech (Regulatory Technology) & GRC software could become a $24bn market place according to industry sources. Regulations are not going away and will continue to grow in comprehensiveness & complexity. Right along with the risk they attempt to responsibly mitigate. We are seeing a huge gap in expertise, those who know what to do with it, how to apply it etc. It's a niche area but with enormous potential.

Advanced authentication mechanisms greatly reduce Personal Identity Information (PII) breach through what's known as Multi-Factor Authentication (MFA). There's a story about Google never having been breached because of their use of Yubikeys, over 70,000 employees have used it. It's a public cryptographic USB solution. Think of it like keys to your house, but it opens up your digital reality. However, one needs backup "copies" as you would for house keys.

The Blockchain or Distributed Ledger Technology (DLT) model, be it as tokens for attaching assets or hyper ledger for fast secure transactions, is quickly being adopted, not just by tech and financial entrepreneurs, but by government entities who are now defining DLT's as evidence and legally binding, i.e. smart contracts and the assets /agreements tied to the DLT. Traditional trade finance processes such as the bank Letters of Credit is being digitalized and the future of most financial assets and exchanges is heading in the same direction.

Space is really the new frontier and the workhorse satellites and data they transmit are the targets. It's still very much early days but we've seen the US government announce space initiatives and as it's own battle domain. In addition to potential kinetic attacks, one could imagine spoofing data links via cyber security technologies. Here is one example, spoofing GPS data is doesn't require one to be up there, just intercept open GPS transmissions.

How important is GPS for everyone? Crucial for our militaries and most IoT applications be it cars or ships rely on it. Not to mention how most people find their way around these days.

Finally, the whole issue of quantum computing and cryptography could turn digital services and cyber security on its head. The ability to iterate at unimagined speeds may overwhelm many of our best protections, including DLT. But that's down the road. We do know China has set national goals achieve dominance in this area so everyone should be keeping an eye on it.

As challenging as these topics appear, we are seeing real benefits through greater productivity and creative solutions coming to the fore in this area. The cloud and evolving security solutions give us "hope" we will overcome and continue to advance.

Q: In the spirit of our love of books and reading, is there any books or writings that you can recommend that has helped form your point of view on this topic?

Erik & Eduardo: Here are some favorites, that are a good place to start in order to get a sense of the future of our digital world and the role of cyber security past and present:

New Solutions for Cybersecurity (MIT Connection Science & Engineering) by David Shrier.

Social Physics: How social networks can make us smarter by Alex Pentland

Countdown to Zero Day: Stuxnet & the launch of the World's first digital weapon by Kim Zetter.

SECURE YOUR FUTURE WITH AN INVESTMENT IN THE KEY COMPONENT OF A DIGITAL WORLD.

INVEST IN CYBER SECURITY...

"One of our core investment tenets is that often the best opportunities are around the edges of things, the more mundane and less obvious, the second-order effects of major trends. Away from the headlines and where you have to dig a little deeper and work a little harder, real attractive risk/reward scenarios can be found."

– Mr. Sune Hojgaard Sorensen, Managing Partner Librarium Associates Ltd.

In a digital world, where the value is in intangibles such as IP and all records of financial assets are digital the real opportunity is in digital/cyber security – as without such measures there is no value plus the co's who have the best process/systems in place have an enormous competitive advantage.

As outlined earlier, according to Ocean Tomo LLC, back in 1975 tangible assets comprised 83% of the S&P 500 market value with the other 17% being made up of intangible assets. By 1995 intangible assets had grown to 68% of the S&P 500 market value with intangible assets down to 32% and by 2015 intangible assets had risen to a staggering 84% of S&P 500 market value. Intangible assets had fallen to just 16% of the S&P 500's market by 2015.

These figures mean that more than four-fifths of the S&P 500's current value is now attributed to proprietary data, human ideas and intellectual property most of which are kept in digital format. It must be noted that the report was done in early 2015 and tech has only gone on to be even more important since then so we can reasonably assume the intangible percentage of the S&P 500 is now above 84%.

As inconvenient a truth as it might be, it obviously means that most of the largest global companies' real assets are vulnerable to hacking for purposes of espionage and/or destructive measures.

We have seen examples of how the market reacts to glimpses of this reality when Yahoo (US) was bought by Verizon, a data breach involving the personal information of over a billion individuals precipitated a discount of about $350 million off the acquisition price and in the 2014 hack of Sony Pictures, when internal emails and proprietary digital property was stolen and leaked to much embarrassment, internal disruption and economic damage tallying up to over $100 million.

In truth much more goes unreported or is only shared once the issue is deemed under control and damage limitation is already underway as with the recent 'NotPetya' attack that partly shut down the sovereign nation of Ukraine and went onto cripple the global operational infrastructure of Maersk, the maritime giant that on any given day is responsible for around a 5th of the entire world's shipping capacity, for several days with an economic loss of around $300 million incurred. The 'NotPetya' attack is estimated to have cost the companies affected around $10 billion. It's examples like this that begin to show us how fragile our digital world really is and how crucial cyber security solutions really are.

Combine that with the increasingly digitalization of the financial markets and the fact that over $5 trillion on average moves around the global economy on a daily basis.

Plus the fact that most of our governmental operative and physical infrastructures such as health records and electrical grids are digital and/or connected. Add how digital communications and social media influences politics and how much the average person now relies on digital tools for their daily lives and you have an incredibly large and crucial universe that can only function if we continue to find solutions for keeping it all secure yet functional.

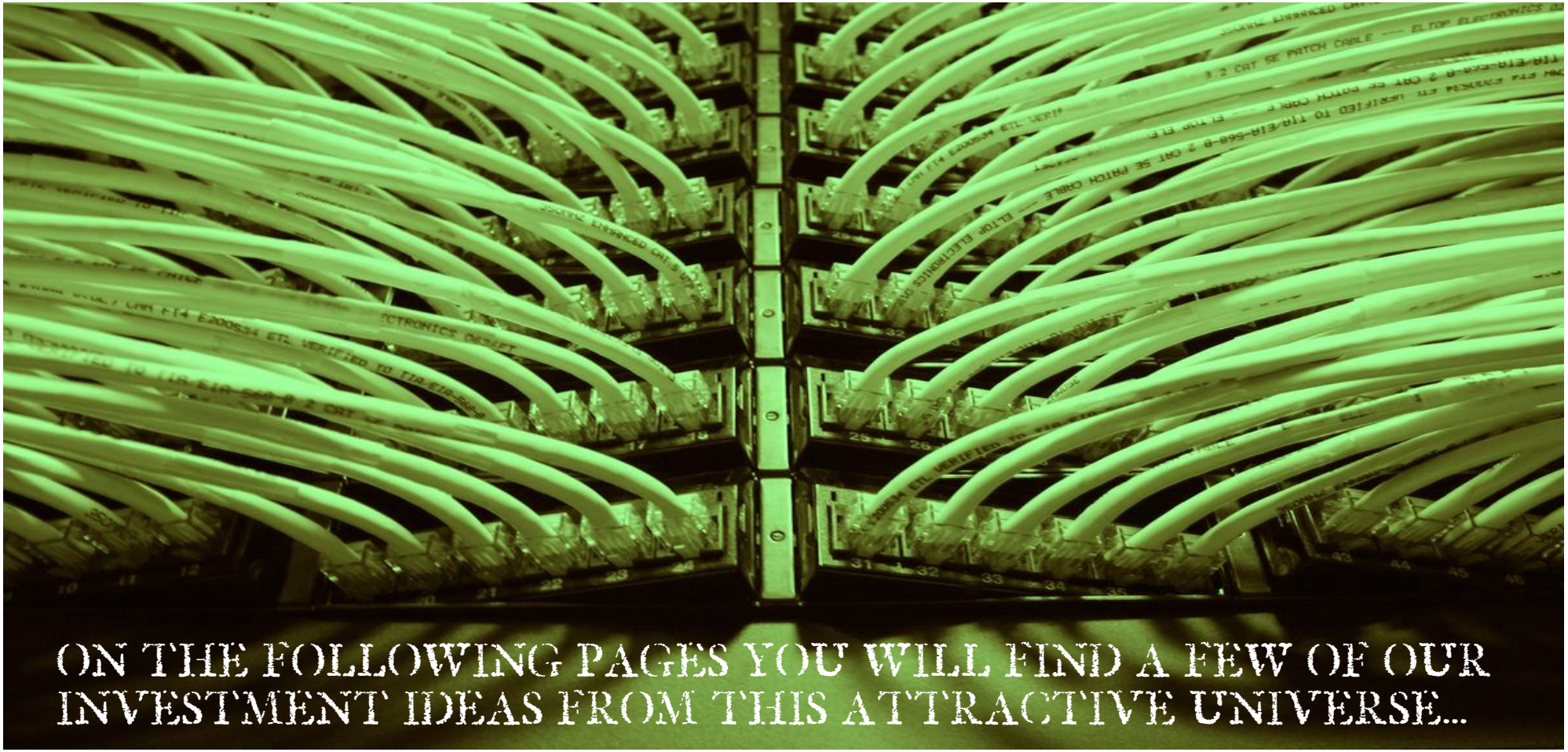
So has the path of progress towards a digital reality outpaced our ability to keep it all secure?

As the 'NotPetoya' event highlights it appears that we are increasingly straining to keep up and the world is speeding up all the time in large part driven by a more hostile reality of state actors acting out of national interests in a coordinated manner and with far more computing power.

A competition or if you like a war is going on in the unconventional spheres of information and cyber warfare, with the US, EU, Russia & China the major players with other smaller players such as Iran and North Korea joining in.

From an investment perspective it is a 'spade and shovels' play - the new 'gold mines' are in digital data and the optimal risk/return approach would appear to be in investing in the security space. It has endless and constantly evolving needs that require solutions from deep pocketed customers.

In a digital world – digital security is the cornerstone & innovative solutions will be the catalysts that facilitates the next stages of development across all sectors of our economic systems. As an investor you will want to stay secure and take part in the growth of this crucial industry.



CYBER INSURANCE: A niche opportunity resides in the 'picks & shovels'.

The world is continuing its digital transformation with no sign of slowing down. The amount of data consumed by businesses increases every day. Companies are also ever more reliant on inter-connectivity of systems and technologies to operate.

At the same time, hackers have become more sophisticated at exploiting networks and software vulnerabilities to achieve their goals and the number of reported cyber-attacks keeps increasing. In addition, the continually evolving technology environment has made it more challenging for companies to keep up with the latest security solutions, leaving them more exposed to potential threats. In this context, the insurance industry will play an important role in helping companies manage their exposure to potential cyber perils.

The cyber insurance market still lingers in its infancy, no one can miss its dynamics. It is the fastest growing line of business in the industry. In just a few years, cyber insurance premiums have grown to an estimated USD 2 billion in North America and USD 3 billion globally.

A combined assault of daily front-page news items about cyberattacks, increasing government regulation and insurance industry awareness are all raising the profile of cyber risk. This is no longer just an IT-based risk but also a major business risk that is being considered at company board and ownership levels. As more regulations are adopted, including global notification requirements such as fines and penalties, the corporate sector is looking to insurance to offer mitigation solutions that can effectively deal with this emerging risk.

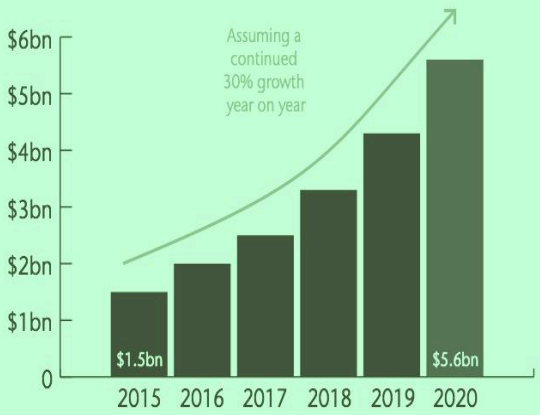
There is indeed a major opportunity for the insurance industry to help mainly corporate and commercial customers better manage and mitigate cyber risks. By doing so, insurers also tap into revenue streams in an entirely new specialized line of business.

From an investment perspective you can look at investing in larger diversified traditional insurers but much of the potential upside will disappear into a broad selection of services. Plus as cyber risk is poorly understood currently, which in turn could pose high risk for insurance companies finding their way in this new treacherous landscape, it may be a better option to look at the innovation going on in the support and operational space for this new & fast growing line of business.

Besides sourcing direct VC style investments in the space yourself, you can look at a small selection of the specialized VC funds for access. We particularly like companies focused on modeling cyber security risks is difficult for insurance companies.

A growing cyber threat landscape and rising incidence of costly attacks makes it increasingly difficult to offer the right cyber insurance packages at the right premiums. Difficulty modeling risk from cyber threats in the commercial insurance business has created opportunities for a growing number of startups to offer security benchmarking, the industry's term for comparing the relative security of companies' networks and systems. Insurance companies can then use these security benchmarking tools to make smarter underwriting decisions around cyber liability. Some startups also provide FICO-like scores around company risk profiles. This is an interesting niche play that might justify the illiquidity and fee related aspects over the long term.

US STANDALONE CYBER INSURANCE MARKET PROJECTIONS...



KEY GROWTH DRIVERS...

Legislation Data breach legislation has been enacted in 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands

Awareness In 2015, US firms ranked cyber as their 5th most important risk, compared to 18th back in 2011

# of breaches More companies are uncovering data breaches and reported breaches in the US have risen by c.325% since 2006

Higher cost On average, the cost of a data breach is 60% higher than it was in 2006

Source: Aon Insurance

TAKING A BROAD VIEW: STRIP MINING THE WHOLE SPACE...

HACK:US

Almost 20 years into the 21st century, we are witnessing the ongoing process of digitization, a world dominated by intangible assets that are generating incredible value and turning industries upside down. Intellectual property itself is digitized, and can be processed, shared, or used freely through digital technology. The percentage of digital communications is growing exponentially and across all segments of our lives. Online is increasingly our reality. At the same time this means a more fragile reality where new and old risks converge.

Cyber security is a keystone in the foundation upon which this new paradigm is being build.

As an investor you should seek long term enduring trends, and identify challenges & bottlenecks that may cause delays or outright limit to this onwards movement. Because it is there that innovation will be needed and the companies, that can solve these challenges will unlock great value and as result should be handsomely rewarded.

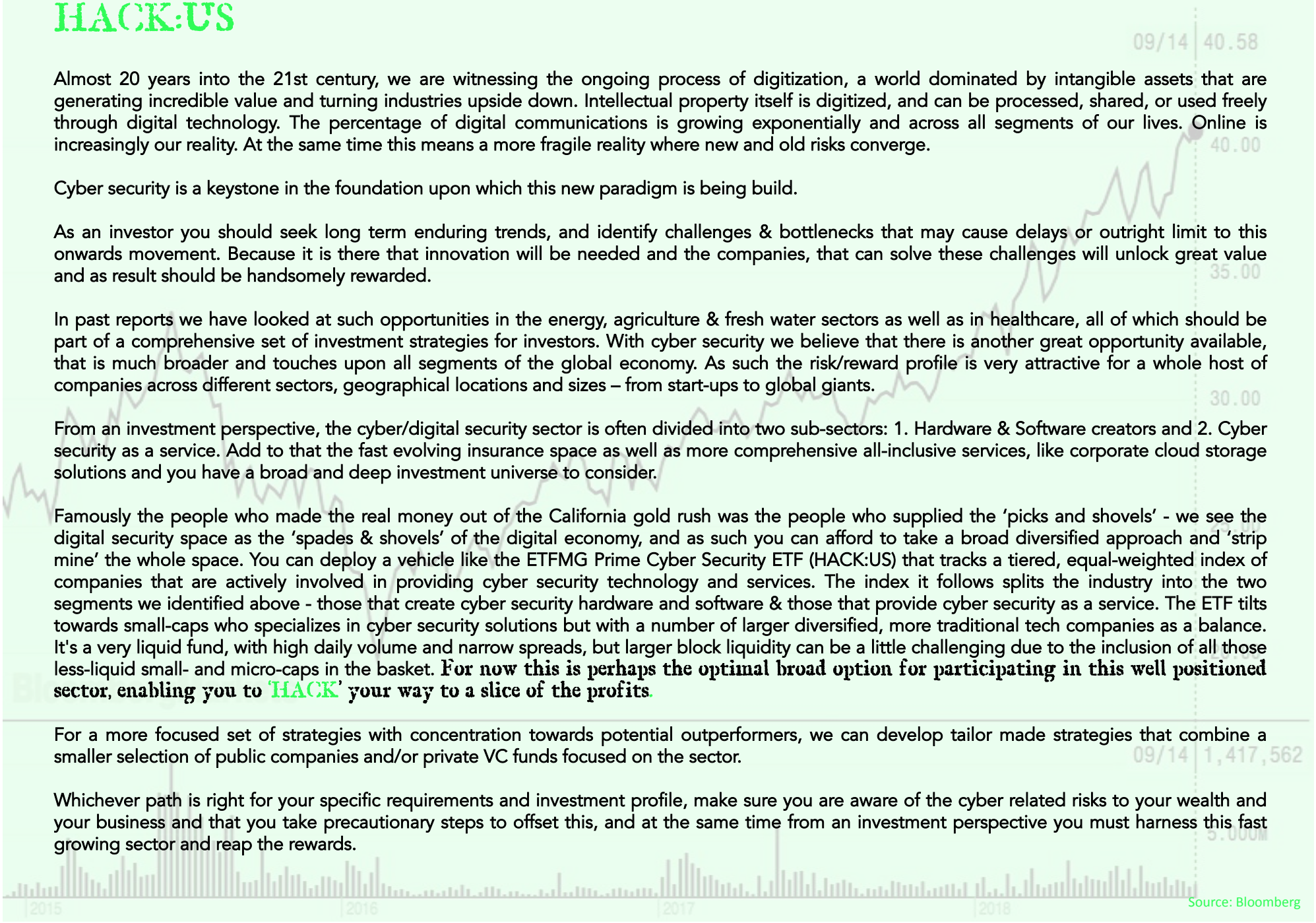
In past reports we have looked at such opportunities in the energy, agriculture & fresh water sectors as well as in healthcare, all of which should be part of a comprehensive set of investment strategies for investors. With cyber security we believe that there is another great opportunity available, that is much broader and touches upon all segments of the global economy. As such the risk/reward profile is very attractive for a whole host of companies across different sectors, geographical locations and sizes – from start-ups to global giants.

From an investment perspective, the cyber/digital security sector is often divided into two sub-sectors: 1. Hardware & Software creators and 2. Cyber security as a service. Add to that the fast evolving insurance space as well as more comprehensive all-inclusive services, like corporate cloud storage solutions and you have a broad and deep investment universe to consider.

Famously the people who made the real money out of the California gold rush was the people who supplied the 'picks and shovels' - we see the digital security space as the 'spades & shovels' of the digital economy, and as such you can afford to take a broad diversified approach and 'strip mine' the whole space. You can deploy a vehicle like the ETFMG Prime Cyber Security ETF (HACK:US) that tracks a tiered, equal-weighted index of companies that are actively involved in providing cyber security technology and services. The index it follows splits the industry into the two segments we identified above - those that create cyber security hardware and software & those that provide cyber security as a service. The ETF tilts towards small-caps who specializes in cyber security solutions but with a number of larger diversified, more traditional tech companies as a balance. It's a very liquid fund, with high daily volume and narrow spreads, but larger block liquidity can be a little challenging due to the inclusion of all those less-liquid small- and micro-caps in the basket. **For now this is perhaps the optimal broad option for participating in this well positioned sector, enabling you to 'HACK' your way to a slice of the profits.**

For a more focused set of strategies with concentration towards potential outperformers, we can develop tailor made strategies that combine a smaller selection of public companies and/or private VC funds focused on the sector.

Whichever path is right for your specific requirements and investment profile, make sure you are aware of the cyber related risks to your wealth and your business and that you take precautionary steps to offset this, and at the same time from an investment perspective you must harness this fast growing sector and reap the rewards.



GET REAL – THE ULTIMATE FAIL-SAFE IN AN INCREASINGLY INTANGIBLE WORLD:

During the research phase for this report and with the conversations with our two experts, Erik & Edurado it struck me that in a digital world, cyber security is crucial but physical real assets are the ultimate insurance.

In a world with around $170 trillion in liquid assets, such as stocks, bonds and currencies that increasingly exists only in digital format, the contrarian option – the ultimate fail-safe is real physical assets, stored outside the financial system in enduring and stable jurisdictions. The obvious option is gold and other precious metals but one could combine it with holdings in forestry and farmland for example.

As outlined in this report and in much of our other work, we are firmly in the camp of believing in mankind's ability to grind onwards with a path of progress and innovation and as such we are not saying to allocate all your wealth to some 'dumb rocks.' However, as a generational insurance policy it makes sense to go counter to the trend and allocate some of your wealth, to that which is tangible in an increasingly intangible world.

As someone explained, in a recent conversation, to a younger person; "**Gold is Bitcoin, for when the electricity is gone and god forbid there is no internet.**" While that is a bit extreme, we certainly embrace a realist approach and if history is a guide, then it often pays to be prepared for the unexpected.

With our partners at www.globalgold.ch we can help you learn more about the optimal set of solutions for ownership of precious metals, with safe haven storage options in Switzerland, Singapore and New Zealand.

"IN ALL CRISES THERE ARE BRIEF MOMENTS OF DECISION WHICH MUST IMMEDIATELY BE GRASPED. ONLY VERY FEW RECOGNIZE THESE MOMENTS, AND THESE FEW INDIVIDUALS ARE HARDLY EVER UNDERSTOOD IN TIME."

– Mr. Felix Somary AKA The Raven of Zurich.

SOURCES & INSPIRATION...

In the words of Sir Isaac Newton: "If I have seen further it is by standing on the shoulders of Giants." On this page we humbly give thanks to those great individuals, source materials & books that provided us with the food for thought and insights shared in this report.

THE REPORTS:

Intangible Assets as a framework for sustainable value creation. – Athena Alliance.

Staying ahead on cyber security. – McKinsey & Co.

How boards can lead the cyber-resilient organization. – Willis Tower Watson & the EIU.

Toward a model for private collaboration in cyber security. – Boston Consulting Group.

Cyber Security: A necessary pillar of Smart Cities. – Ernst & Young.

Chinese Cyber espionage originating from Tsinghua University infrastructure. – Recorded Futures.

2018 Data Breach Investigations Report. – Verizon Research.

Industrial Control Vulnerabilities: 2017 Review. – Dragos Inc.

Cybercrime-as-a-Service: Indentifying Control Points. – MIT ICICIC Study.

Global Cyber Market: Uncovering the hidden opportunities. – Aon Insurance Research

Cyber Insurance as a risk mitigation strategy. – The Geneva Association.

Analysis of the attack on the Ukrainian power grid: Defense Use Case. – E-ISAC Study.

The cost of malicious cyber activity to the U.S. economy. – The Council of Economic Advisors.

If you go read one article, go read the illuminating & deeply concerning:

The untold story of NotPetya, the most devastating cyber attack in history. By Andy Greenberg.

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

ABOUT LIBRARIUM:

Librarium Associates Ltd. is an independent research company focusing on global macro and geopolitical monitoring and analysis. We are committed to delivering distinctive insights on global trends enabling our partners and clients to make in- formed decisions in a changeable world.

investors with monthly and quarterly publications providing an independent overview of global macro economic and geopolitical events and their implications on the world of investing.

We also provide intra-monthly event driven insights as a part of our constant horizon scanning services.

Our services can also be employed on a retained basis, providing the client direct & always confidential access to our team on an on-going basis allowing us to act as an independent sounding board for our clients ventures.

We prefer to work with a relatively small and select group of active clients allowing us to provide them and their projects with our full attention and as such we operate a limited amount of such partnerships.

Contact the Author: shs@librariuminsights.com
Visit & Subscribe: www.librariuminsights.com
Converse with us on Twitter: @LibrariumViews