ISSA Cyber WG Workshop

June 17, 2026

Workshop Minutes / Notes

Alexander	Boesch	SIX
Bill	Hodash	ISSA
Charlies	Clarke	Thomas Murray
Edward	Starkie	Thomas Murray
Fiona	McNally	BNY
Gary	Delaney	BNY
Giles	Elliott	TCS
Joris	Pinjoy	Euroclear
Julia	McKenny	ISSA
Juliette	Kennel	SWIFT
Laure	Moliner	Euroclear
Oliver	Dazard	SWIFT
Shreej	Joshi	Thomas Murray

Welcome

Charles Clarke welcomed the participants and set some context:

- The timeline for an attacker to implement an attack strategy following discovery of a vulnerability has shrunk from 23 days to now 15-20 hours and with a 76% success rate. The question for 2018 must change from how we protect our financial infrastructure to how to we fundamentally change the way we run our businesses to be resilient in this new environment, moving from command and control to continuous control.
- It was clear from the context setting that the world has significantly changed since 2018 and in the Executive Summary we need to sum up what all the changes to each section of the paper means for the industry and its structure. What does the industry look like if all the investments are made by all industry participants?

2018 Paper Section 2: Threat Landscape

- The main change since 2018 is the speed of attack and thus the need for much more rapid attack response.
- The revised section should start with the players and their motives before moving to attack techniques.
- It was observed that the expected cyber warfare (on wider industry) did not occur during the Iran war and that may have been that Iran viewed cyber-attacks on infrastructure of its enemies as a true last resort tool to be used only to defend against collapse.
    - Attacks on organizations in region were detected both in US and Iran, several Iranian banks impacted at the same time.
    - Physical/ Kinetic attack on data center impacted organizations in the region (I think it was an AWS DC).
    - Possible that attacks on supporting infrastructure could take place.
- Theft from the financial industry is not a prime motivation.
- We should add to the paper:
- Disinformation campaigns as a key attack tool.
    - Can be related to cyber-attacks (HSBC – Central America), individuals, businesses.
    - Generate overhead and need to provide correct narrative, spooking markets possible etc.

- Use of open-source software as a key potential vulnerability as it drives more risks, and we have seen a number of attacks in this space, sometimes involving the positioning of a threat actor for several years in opensource code repositories.
- Use of AI as a means of quickly developing hacking tools, and supporting the review, processing, and use of data for rapid analysis.
- Geopolitics as a key consideration (the US has a frontier model and is in control of it).
- This has changed in recent weeks where the Chinese have spoken about their own version of Mythos.
- The risk mitigation framework must be continually updated and the use of AI to achieve that.
- The revised paper should be structured in a way to be more quickly updateable with links to the most current data.
- More focus on third party (and fourth party/fifth party) partner concentration issues and the risk of sleeping code embedded in large players. Focus on Cloud provider concentration issues including Geopolitics (again, U.S. control). Bad actors will go after the supply chain, look for the concentration points to the most key players – third party providers must change their operating models in response to the increased threat to them. Need for 3rd parties to make clear notification protocols in Contractual Terms and this may conflict with regulations requiring confidentiality and slower disclosure. Banks need to be able to switch 3rd party providers intraday. Is there a role for ISSA here in making clear the risks of a lack of harmonization on breach disclosures are?
- Wider consideration is the impact that politicization of technology and data/ technology sovereignty.
  - Existing tech must accommodate, key parties in the market may be requested or encouraged to use local players, EU is particularly seeking to build “Digital EU”.
- The need for Intraday patching changes the way you run your business including the need to test intraday before running patch into production.
- Automation is a key consideration here, unable to patch at the speed required manually.
- Vulnerability Testing needs to be much more exhaustive – the business risks have changed, and the ROI of more testing has increased. We must invest more upfront to avoid exploitable software moving into production. This will likely require embedding in additional controls into the Software Development Lifecycle (SDLC).
  - Vibe coding also increases the volume of applications or inhouse developed applications in particular which are unlikely to have tested during the SDLC to the same extent as standard/ traditional applications.
- Raise the question as to whether software liability must shift to have more balance between providers and customers.
- AI will allow software development to speed up rapidly, but we may need to slow down implementation to provide for significantly more testing.
- Does the Availability/Integrity/Confidentiality Model need to shift?
  - It is also likely that CIA will not apply equally across supply chains.
- Should we add a primer on “Firewalls” and what they mean in the current environment?
  - What is the role of traditional secure enclave thinking regarding hardened permitter?
  - Zero trust could be the replacement, wider lauded etc.
- General digitalization as a shift in trend from previous paper, greater demand for more ways of interacting, processing data, more interfaces, data exchanges, applications architecture and designed to be integrated and share information, supported by regulation to support competition in the Financial services industry generally.
- 2018 – things changed and upgrades had to be done on an annual budget cycle whereas now this needs to be done on a continuous basis – CEO level decisions/focus, constant funding models.

- Concentration risk – we all have it via use of common CSDs in markets and impact of cyber-attack on one of them. Impact of AI
- Our ability to assess counterparties who say they cannot reveal their security protocols due to confidentiality reasons especially where they have a monopoly
- Weakest link of 3rd/4th parties who just don't invest in upgrades/patches etc
- Moving to Continuous evaluation model as opposed to look back DD
- Disconnection/reconnection protocols with 3rd parties

New Section: AI and Quantum Computing

Gary presented on Mythos as BNY is open of the firms included in Project Glasswing.

- Mythos was not developed as a security tool. The vulnerability discovery capability was discovered by accident.
- Mythos can identify vulnerabilities that cannot and have not been detected by other tools and goes further to finding ways to exploit them incredibly quickly, by looking deep into the code of applications. Mythos proves the vulnerability by determining successful exploit methods. Mythos also chains together many low-risk vulnerabilities into a cumulative high-risk vulnerability with successful ways to exploit all the vulnerabilities in aggregate. A low classified vulnerability might mean critical if it can be used as part of the chaining attack.
- Mythos is challenging to get up and running in that you need to implement guardrails surrounding it.
  - High degree of technological maturity, governance and oversight required to do this- this level of oversight is unlikely to be as rigorous across all future users. High level of risk for businesses that do not do this but also organizations in close technical proximity to those that do not.
- Mythos works most effectively with the least specific prompts, which is too risky for banks, thus requiring both more specific prompts as well as the extensive guardrails.
  - Liability related to these toolings could be an issue if they are used for testing and
- Mythos performs both Static Scanning and Dynamic Scanning on your computer code in production and it will find many items to fix, some of which are exploitable and others that are not. Large commercial software providers like Microsoft have found literally hundreds of exploitable vulnerabilities in the code of their core applications provided to businesses and consumers. As a result, they are issuing more patches than ever, more quickly and often than ever.
- Firms using Mythos are often finding many low-level vulnerabilities in their own code and in aggregate they do lead to a higher risk.
- Mythos characterizes the nature of each vulnerability, and each firm needs to feed each through their own risk assessment framework.
- Mythos is non-deterministic. You need to ask it, get results, ask it again, get slightly different results - - so keep doing it - -
  - This practice might not be adopted by other organizations due to cost implications and their own risk/ cost appetites.
- Mythos writes the code to fix the vulnerabilities, making them ready to be checked and thoroughly tested before being installed. Many of these vulnerabilities are in applications in old programming languages, making checking and testing challenging.
- Geopolitics – Clearly Anthropic is in a struggle with the U.S. government and the government has just invoked export controls. Open AI's models are catching up, but they are a U.S. supplier as well. Will the US invoke national security risk controls on them as well?
  - Comparisons between AI and the attempted introduction of export controls to cryptographic algorithms in the 90(s) could be drawn.

- Costs – The compute tokens that allow you to run Mythos queries in this fashion can be very expensive. One of the 40 Project Glasswing firms is reported to have spent $500 million already. The AI companies right now are a monopoly/oligarchy and while you need to develop a framework to efficiently use them, in the end there is no alternative – you must pay.
- While Firms cannot legally use Mythos to find vulnerabilities in commercial software, the expectation is that the vendors will and that soon the regulators will require all vendors of software used by the financial industry to use such AI tools to find and fix the vulnerabilities in their applications. This a key development that ISSA can bring attention to.
  - An issue may arise where vendors either do not have access to the technology of cannot afford to use the technology.
- Industry Structure Issue – might the investment required to remediate and stay resilient using such tools challenge the profitability of the securities services business for some medium and small players and lead to another wave of consolidation?
- Agentic AI: What are the impacts of one firm's agents interacting with transactions with other firms?
  - It is an extension of the insider threat risk which is a term that is understood by organizations, it is however hard to address and is often poorly managed by them, if at all.
  - Some members are already using agentic AI with users having phone numbers, inboxes etc. to interact with.
- ISSA may want to stress:
  - The need for sharing scanning/remediation results
  - The impact on 3rd parties and 3rd party risk management.
  - That regulators can help by imposing requirements on 3rd party providers that gain revenue from the financial services industry.
  - A position on whether DORA is good/ bad, etc. as it does place an extended focus on third party risk
  - The impact on Board Governance – insisting on finding and fixing all vulnerabilities regardless on short-term impact on earnings and opportunity costs.

2018 Paper Section 3: Risk Assessment (of the Securities Services Industry)

- Consider placing more emphasis on stealing inside information and the overall connectiveness of the industry players to market infrastructures, third parties and each other. Include the risk of simultaneous attacks on key suppliers (e.g., Cloud suppliers) at any time but also during other stressful events including a financial crisis or highly volatile trading days. Include malicious insiders at key 3rd party suppliers.
  - Previously some technology suppliers have been seen as too big to be insecure or unreliable, this attitude cannot be allowed to exist without being challenged appropriately.
- Increase emphasis on Geopolitical issues including sanctions and the impact on the broader industry. Focus on motivations of bad actors and why Capital markets and Securities Services may be a target for those with certain motives.
  - Finance classified as CNI.
  - Operations required for normal society to operate
- Should we call out that there has been good progress on transparency on attacks but not on risk mitigation? Focus on systemic risk, reputational risk, faith in Capital Markets.
- Perhaps tie misinformation campaigns to manipulated prices.
- Has something changes since 2028 that calls into question the back-up schemes, we have today? Has the business case for deeper resilience changed? Do we need improved systems to identify anomalies and potentially discover and diagnose potential attacks sooner?

- How does the advent of Digital assets impact the industry's susceptibility? Are there new key players (both regulated and unregulated) in Digital Assets processing that can be compromised by attacks, and would that spill over into the broader Capital Markets?
    - In addition, are traditional players who use new players (third parties) best positioned or aware of the new technologies that could be required to support new approaches and are being used within smaller/ more dynamic orgs?
    - How to encourage innovation internally and within third parties without stifling it?

2018 Paper Section 4: susceptibility of Securities Participants

- Is there a geographical consideration on Custody Risk?
- Should we consider deleting Figure 6 and replacing it with an analysis of the impact to the whole industry of a key player in each of the segments being taken down by an attack e.g., Whole industry use of Cloud; e.g. MS / Use of Canton Network by key infrastructure, what happens if Canton network goes down?

2018 Paper Section 5: Existing Regulations and Frameworks

- Start with New Regulation (both domestic and international), then updates to the Frameworks (e.g., adding Governance to NIST), then more adoption of the MITRE framework - - point out the need to map your own bank's framework to MITRE.
- Show that the cost of compliance going up and demonstrate that this can be considered as smart investment reducing risks.

2018 Paper Section 6: Recommended Risk Mitigation Practices/Internal Controls

- Link these back to the threats and to the frameworks
- Add Zero-Trust Principles:
    - Never Trust
    - Assume Breach
    - Separation of Duties
- Much more segmentation and components allowing compromised components to be shut down without shutting off whole products or services.
- Show the evolution from focus in 2028 on prevention to current focus on corrective controls/restoration.
- Consider adding a focus on Reconnection protocols (for this paper or a follow-up paper).
- How far down the chain should the revised Third-Party Risk Management sub-section go?

2018 Paper Section 7: External Framework Elements and Approaches

- Consider eliminations sub-sections 7.1 (Alternative Enforcement Approaches), 7.2 (Implementation of a Risk-Based Approach), and 7.3 (Three Lines of Defense Risk Management Strategy) and keep 7.4 (Recovery from a Cyber Attack - - see above discussion of adding Reconnection protocols).
- Add discussion of the need to connect to all aspects of security for a firm.

Appendix 1 – Use Case "SWIFT Customer Security Program"

- Add increased involvement by Certified Assessors (being phased in over 3 years) as well as increased engagement by Supervisors
- Add additional critical controls and escalation of penalties
- Link ISSA paper to the most current version of CSP and keep that link current as changes are adopted.
- May all new changes to CSP to revisions made to the seven sections of the paper.