The Multinational Company Perspective on Multi-Stakeholder Trust and Transparency

DXC Technology Company (“DXC”) is a technology service provider located in over 70 countries. We provide IT services globally to thousands of customers, including to over 240 customers in the Fortune 500 and to a number of national governments. Services provided to customers include cybersecurity, but DXC also maintains a robust cyber program designed to protect its own internal systems, applications and proprietary data worldwide. At DXC, we firmly believe that we have a responsibility to be actively improving and challenging the tech sector and governments in order to facilitate a secure environment for NGOs and other stakeholders. We also believe it is critical that the private sector engage with international stakeholders as governments and their constituents work to establish international norms, laws and regulations applicable to cyber events. Accordingly, we have actively engaged as informal participants in the Open-Ended Working Group on Security of and in the use of Information and Communications Technologies (OEWG) since 2019 and have been an active contributor to the Paris Call for Trust and Security in Cyberspace, as well as other industry interest groups and consortiums.

As an NGO supportive of the success of the OEWG and especially grateful for the OEWG’s role actively seeking to bringing industry and government together, we submit this Intervention and identify three points immediately worth noting: First, in the relationship between industry, government, and NGOs, trust is absolutely critical. DXC believes that every entity must be open in its dealings and should expect the same from others. Second, we need to be transparent. Because our clients and customers make up a sizeable part of the global population, we need to be transparent when we face attacks and in how we respond to attacks: no-one is made stronger by our fear to expose ourselves. Third, we cannot be complacent. The threat of ransomware and other cyber attacks has certainly not gone away. With these messages in mind, DXC would like to contribute learnings from its own cyber attack experience. DXC will outline an example of a very real attack as a case study which emphasizes the need for government and all Stakeholders, including industry, to work together.

A Ransomware Case Study on Trust and Transparency:

On July 4th, 2020, a subsidiary of DXC, Xchanging, which provides technology-enabled business services to the commercial insurance industry, was subject to a ransomware attack. Xchanging plays an essential role in UK Critical National Infrastructure due to its significant work with the London Markets. While Xchanging’s business is segregated from DXC’s larger IT network, our specialists were concerned about whether the incident would have operational impacts on Xchanging and the wider company. The attack took place on a Saturday, with a very real risk of operational impacts to customers when the markets opened on Monday.

The attacker had sent the following message: “We have your data. We’ve encrypted your files. If you want to negotiate, we can talk on a secure tool or chat session.” Our work ensured that engaging with the attackers was not necessary. Our team of specialists and experts worked through the weekend to verify that no data had been stolen, that only a handful of non-critical systems had been accessed, and that we were able to rapidly neutralise the threat.
On Sunday, we were able to fully clean and restore the impacted environment. By Monday morning, Xchanging and the London Market was able to open as planned and process global insurance policies and transactions. Critical to our success was trusting our governmental support and customers rather than working to resolve in a silo. Instead, we contacted and engaged the appropriate authorities and our customers early and with candor.

Too often, companies suffer ransomware attacks and engage with the attackers while withholding information from the authorities and their customer base. Legal counsel often advises this caution. Transparency is vital for creating trust for the wider supply chain and ensures that other companies can learn best practices from our steps to resolve the incident.

DXC identified five crucial lessons for consideration by multi-stakeholders including two of which are relevant to truth and transparency:

1. **Know your infrastructure.** Ensure all networks and firewalls have enterprise security tools in place to detect malicious behaviour. We were attacked using “Cobaltstrike”, a publicly available security testing tool. Knowing our infrastructure ensured that we were able to quickly detect when something was not right and identify where the network was compromised.

2. **Involve senior leadership from the outset.** We are a global company, spread across over 70 countries. To take rapid action, we would need to deploy staff in both the United Kingdom and India and engaging leadership teams was naturally critical. Good and tested governance, accountability, and clarity was essential.

3. **Engage authorities and experts early.** The attack took place on a holiday weekend in the USA (Independence Day). We had identified that the ransomware threat actor was utilising website domains in the United States to facilitate the attack. Good relationships ensured that we were able to contact law enforcement officials working on the holiday weekend, and we obtained a court order to take control of the attackers’ internet domains by that evening.

4. **Gain leverage and do not pay.** Our attackers wanted to negotiate; often, they will ask for money upfront in difficult to trace payments (cryptocurrency). We identified our strengths early: we knew we had stopped the attack; we knew they did not have our data, and we knew we had backups.

5. **Be transparent.** Openness is good practice. We shared details of the attack with hundreds of customers worldwide as well as several authorities in different jurisdictions. Medium to long-term, this has ensured that we continue to be regarded as a trustworthy and sincere company. In the short-term, it enabled us to move openly. An attack over a weekend is problematic; over a holiday weekend and it could have been critical. At the time, the average ransomware attack took down critical systems for sixteen days. Our transparency enabled us to move quickly, and it was resolved in time for markets to open on Monday.

The lessons outlined were important responsive actions that leveraged both acting preventatively and proactively. Companies like DXC are reliant on their entire supply chain (including experts and the government) implementing appropriate hygiene in their work.

Ransomware is a threat on a global scale. Increasingly cyber-aware groups and individuals can source ransomware tools with ease online and deploy them against companies and individuals at an unprecedented pace and scale. Public services across the world are especially at risk due to often running
legacy IT and employing staff who, naturally, have responsibilities that preclude them from upskilling themselves digitally.

Perhaps most alarming, however, is the potential for nation-state attacks. The Ransomware Threat Assessment Model (NCSC-A/R/1197-22) identifies the 10 most prolific and dangerous ransomware strains. Nine are likely based in nation States (including Conti, regarded as responsible for the 2022 NHS attack). Seven of the ten have hit UK sectors in the past six months, including: technology, education, manufacturing, charities, transport, legal, financial, and academia. It has long been speculated that these attacks are endorsed by a specific nation State, highlighted by increased attacks in the build up to the invasion of Ukraine (none more notable than the 2017 NotPetya attack which caused havoc for Ukrainian critical national infrastructure). Indeed, NotPetya has been described by multiple outlets as an act of cyberwar. It had worldwide impact as unpatched systems were vulnerable to EternalBlue (an exploit also used in the WannaCry attack).

Modes of extortion are also becoming more challenging. The rise of cryptocurrency as an alternative payment, and one which is not tethered to any central bank or national currency, has created a ransom that is incredibly difficult to trace. This encourages gangs and individuals to target as many computers as possible in attacks, to maximise revenue. Extortion methods are, in turn, becoming more complex. Our personal experience, in 2020, saw the attacker gain access to a subsidiary’s minor database and use that to attempt a ransom negotiation. The WannaCry attack saw computers themselves locked out in exchange for a payment. These forms of extortion encourage business to “lockdown” and not communicate externally, which then feeds into a cycle of success for the attacker. At DXC, we encourage businesses to learn from our experience: appropriate, prompt communication and transparency was key to our success. Indeed, we recommend this blog series on our approach to security.

International Lessons and The Drive for Cooperation through Trust and Transparency.

DXC’s response focused on attacks from criminal gangs and individuals. To maximize global security, trust and transparency must exist across all stakeholders. The public sector, States and NGO’s including industry, UNIDIR, OECD and the OEWG are effective resources for co-ordinating governments and large private sector companies to discuss emerging threats and how to respond. Individual States play a significant role in global cooperation and can lead through developing trust and transparency with Industry. For example, the UK Government has empowered the GCHQ, and others to engage with the private sector to continue sharing learnings and developing generally accepted best practices. Collectively these organisations need to ensure messages are cascaded appropriately and continue to work with NGO’s including industry in forums such as OEWG informal sessions.

Conclusion

An effective multi-stakeholder security program can be enhanced through the practice of the three proposed tools proposed in this contribution, trust, transparency and avoiding complacency. Our cyber attack hit at the worst possible time for an American-owned company: 4th July weekend. Staff were enjoying the national holiday for not only DXC but, crucially, regulators and clients. However, we had actively pursued relationships with the right regulators in relevant markets. DXC could stand up a response, as part of our tried and tested planning, on the worst possible day with great success. Regulators
knew that, when we came to them and told them what we needed, or when they asked us to do something, **we were trusted to give them all the information.** We also trusted them to only ask for something that they genuinely needed. Secondly, we were transparent. The global insurance market could have been heavily exposed when the markets opened at 9:00 am on Monday. **We were transparent with our clients and, importantly, on social media.** Clients, prospective clients, and citizens were aware of what was happening and, importantly, our action to resolve the attack. Resolve it we did. Finally, this proves that **complacency cannot be allowed in government or in industry.** The market indicates there is no sign ransomware and similar attacks are over or substantially diminished. The impact of that one attack, had it worked, could have been devastating for companies and citizens across the globe. With millions of attacks undertaken globally every day, including by state-backed actors, the old saying is worth repeating: it only takes one to succeed.

DXC believes that we have a responsibility to challenge us all to be better. Multi-stakeholders, including industry, working together, have the right people to achieve success. With multi-lateral trust, transparency, and addressing complacency, together we have the ingredients to succeed.