March 2017

THE KOSCIUSZKO INSTITUTE

THE KOSCIUSZKO INSTITUTE POLICY BRIEF

Ahmed Aldoseri, Adam Palmer

Successfully Creating & Leading a Large National Cybersecurity Programme

authors

Ahmed Aldoseri – CISSP, is a Bahraini cybersecurity and cyberlaw expert. He is credited with establishing Bahrain's national CERT, championing several local laws including cybercrime, freaedom of information, and data classification, and leading development of Bahrain's Cyber Trust Programme. Ahmed holds a BSc in law (Hons) in addition to several professional certifications, and was recognized amongst the best 100 CISOs in the Middle East in 2016 within the category of 'Government Security Leaders' by the CISO Council.

Adam Palmer – CISSP, JD, MBA, is a global cybersecurity policy and strategy leader. Adam is a former US Navy Officer, Prosecutor, and Manager of the U.N. Global Programme Against Cybercrime.

Creating a large complex cybersecurity program is one of the greatest challenges organizations can face. It requires investment, vision, planning, and leadership. It also takes commitment. The commitment to start a multi-year program and see it built from design thru to successful implementation.

The Bahrain Cyber Trust Programme is an example of a national cybersecurity program implemented successfully. This case-study can serve as a successful model for global professionals improving cybersecurity.

The Bahrain Cyber Trust Programme: Overview

The Cyber Trust Programme is a framework of procedural, technical, and policy requirements to be implemented by government entities to enhance trust in the government's electronic environment and in its management of citizen data. It sets out cumulative requirements that must be met to progress from one 'trust' level to another, with trust levels starting at *Practitioner*, moving up to *Progressive*, and finally reaching the *Expert* level.

In assessing the existing security environment of Bahrain, it was determined that there were varying approaches to protect the confidentiality, integrity, and availability of data, which produced inconsistent results and, at best, created 'pockets' of good security practices. This left much to be desired. One of the first challenges was raising awareness amongst government users of the threats that target them daily. The Cyber Trust Programme aims to address this knowledge "gap" by creating a culture of cybersecurity awareness and safe practices. It provides government entities with clear strategic and operational targets to achieve. Another unique feature is that the program fosters a sense of competition between government entities to achieve better results and higher certification levels.

ISSN 1689-9873

Building the Right Team

"First *who*, then *what*: 'It's not just a business principle, it's a life principle' … Get the right people on the bus" — Jim Collins, *Good to Great* (2001).

Jim Collins published his best-selling business book *Good to Great* in 2001 and emphasized a key for successful organizations is to bring together the right team. As Collins noted, "the executives who ignited transformations from 'good to great' did not focus on 'where to drive the bus' and then get people to take it there. (…) no, they first got the right people on the bus — and the wrong people off the bus. Then figured out where to drive it (the strategy)."

The good-to-great leaders understood three simple truths.

- If you begin with "who", rather than "what", you can more easily adapt to a changing world.
- If you have the right people on the bus, the problem of how to motivate and manage people is easier. They will be self-motivated to get results.
- If you have the wrong people, you will fail. As Collins notes, "Great vision without great people is irrelevant."

It is important to understand how Bahrain recruited its security team, developed their capability, and inspired them to execute his vision.

As Collins noted, "the executives who ignited transformations from 'good to great' did not focus on 'where to drive the bus' and then get people to take it there. (…) no, they first got the right people on the bus – and the wrong people off the bus. Then figured out where to drive it (the strategy)."

When the Bahrain CISO took his position, he was fortunate to start with a good core of people. They were very highly trained and motivated but lacked direction and coaching. The CISO focused initial efforts on giving the team members a purpose. Uniting them behind a mission that they could relate to and strive to achieve. The purpose was simple: to maintain continuity of government. This was broken down into strategic goals and operational targets that can be tracked and tweaked as we evolved.

The CISO also challenged the security team to be the best at what they do. Aside from operational excellence, each team member was required to acquire or renew professional certifications as related to their field at least once in a 2-year period. Promotions were tied to these achievements which further incentivized staff to develop themselves professionally.

Another important aspect of team development is being able to show the team the results of their work. In cyber security, teams can become overwhelmed with security incidents. This can easily cause the team to lose focus of the big strategic picture. Bahrain's team dedicated time to establish analytical baselines and regular updates to statistics to show the team the results of their work. This leads to a feeling of gratification and achievement. The team could clearly see progress towards the lager goals.

Creating the Vision

The Cyber Trust Program ("CTP") is a vision for improving the cybersecurity maturity of all Bahrain government entities. The Plan encourages government entities to enhance information security, utilize cyber threat intelligence, and build a successful cross-government defense in such a manner that enhances the overall security posture of Bahrain.

The goals of CTP are to provide an operational information security framework that raises the level of information security through the support of human, technology, and procedural elements. This results in a trusted cyber environment for the government that also supports regional and global leadership in cybersecurity. CTP is designed to:

- Assess information security maturity at government entities based on established standards.
- Define a roadmap of requirements for maturity levels that are verifiable, and enable government entities to evaluate and progress towards an acceptable information security posture.
- Encourage and provide a framework for development of threat intelligence and cross-government threat information sharing.

- Establishes a mechanism for evaluating government entities with the requirements at each maturity level of the program. Government entities will be placed at a maturity level based on initial capability assessment and supported on a roadmap to reach the highest level appropriate to the necessary risk posture target.

CTP is designed to enhance Bahrain's position locally, regionally, and internationally in the field of information security, through ensuring that well-defined processes are used in the governance of information security, and continually sharing intelligence information across government entities. This program provides a structure for evaluating information security practices at government entities based on well-defined and clear standards, conditions, and best practices, leading to the achievement of desired goals of information technology security.

Bahrain recognized that traditional approaches to protecting the confidentiality, integrity, and availability of information provide a good foundation for security, however, there are other requirements to achieve a higher level of information security maturity. The creation of a harmonized cross-government culture of security is critical to achieving a holistic "adaptive defense".

CTP encourages government agencies to raise the standard of information security through the application of best practices, technical solutions, and intelligence-based security methodologies that focus on preparation, detection, and response rather than solely prevention. To achieve cross-government harmonization, the program's framework was aimed at assuring information security in all government entities in a uniform manner that also accounts for the differences in risk and security environments across the Bahrain government. Rapid sharing of threat information creates threat intelligence to prevent a cyber-attack from becoming a major security incident across the government. CTP provides a basis for government entities to develop their infrastructure, train their staff, and encourages a culture focused on information security, while also encouraging positive competition for advancement within the framework and gaining recognition.

A question arose during development of the program's initial structure as to whether the program should have a single or multiple certification levels. Specifically, should CTP follow the example of other standards in either granting full certification to a participating entity or reject certification altogether? Bahrain found that such certification models discouraged government entities from endeavoring to achieve standards compliance as the effort required to meet all requirements of a given standard can be daunting. The Bahrain government therefore opted for a multi-tiered structure that allows for developing entities to quickly achieve at least the most basic level of program certification, and allows for more advanced government entities to take on the more rigorous requirements of higher levels.

Within the requirements of all maturity levels, CTP was designed to support the process of developing and providing government services in a secure manner that will earn the trust of end-users and improve their confidence in the safety of their data.

By providing three levels of maturity requirements, CTP gradually raises the level and maturity of information security practices at government entities through carefully planned stages, which directly serves national strategic goals in managing information security, while simultaneously developing national capacities and expertise in information security. Within the requirements of all maturity levels, CTP was designed to support the process of developing and providing government services in a secure manner that will earn the trust of end-users and improve their confidence in the safety of their data. This is anticipated to have a cascading effect on raising usage levels of electronic services, thereby improving quality of life for citizens and residents.

At the heart of the program is the concept of continuous improvement. Government entities are challenged to achieve greater and greater levels of maturity and are allowed the opportunity to self-assess their compliance several times a year before an external audit is conducted to award or renew certification. This process of continuous improvement is essential for any organization to meet the challenges of emerging threats and to ensure that the CTP's requirements are upheld on an on-going basis and not only at audit time.

Getting Leadership and Cross-Government Support

Successfully driving an executive board leadership discussion on information security is critical for success. Security Leaders must be prepared to identify the threats, outline the reasons for building the security program, how they will reduce risk, and overcome the challenges. The board meeting should be a collaborative process that pulls together cross-sector partners for support.

Once a leader decides "how good they need to be," the leader should adopt a policy based risk management approach. Oversight of the technical security process may be led by the CISO, but the CIO can drive a cross team collaborative approach. Security is a process. It requires a governance structure to serve as the support mechanism to steer the program and resolve critical decisions. Having cross-functional support greatly helps in justifying policy change, and budget you may require or success.

The area of public-private partnership, including cooperation with industry partners, the financial sector, academia, and law enforcement, plays an important role in increasing cyber security and resilience through raising awareness of threats and preparing adequate support for an effective response.

The main areas are:

- Law enforcement partnership (including reporting, prevention, deterrence, disruption, investigation, and victim support).
- Cooperation with third parties, including industry (examples are awareness campaigns, promoting security by design, security by default and privacy by default, and tool development).
- Communication channels for the secure and lawful exchange of information and intelligence with relevant partners.

When it comes to detecting and preventing cyber attacks, the cliché "it takes a network to defeat a network" is often used. Given the borderless, asymmetric character, volume, level of sophistication, and financial impact of these attacks, cooperation of all stakeholders at national and international levels is key to success.

Challenges

Several challenges were identified during planning and designing the Bahrain Cyber Trust Programme. Any of these concerns could have caused the Bahrain programme to fail. These challenges included:

Challenge 1: Why should the Bahrain government develop its own information security framework instead of adopting an existing one?

Bahrain addressed this challenge by surveying government entities and gauging if, and how effectively, government entities adopted pre-existing information security standards. The answer was: not many, and not very effectively. The main struggle faced by government entities was the amount of time and money required to be invested in order to achieve compliance with a given standard. Furthermore, current standards did not allow for partial certification or several levels of certification, which were identified as a key selling-point with government agencies.

Challenge 2: How can the program development team get buy-in from Government entities to participate?

The CISO addressed this challenge through an inclusive approach. All program documents were prepared for a detailed and lengthy consultation period, during which government entities had the opportunity to fully communicate and help shape the program. The program development team was surprised by the level of participation and by how quickly the program became a shared idea.

Also, a mechanism was built into the programme for recognizing achievers and honoring their efforts. The program has a recognition process in which the awards are given out to the highest achievers for each maturity level, the highest improvers, the best awareness campaign, the government cyber security professional of the year, and others. This helped encourage participation and reward efforts.

Challenge 3: How to fund the program?

This challenge was addressed by evaluating current expenditures of the government and comparing such expenditures with what CTP would potentially add. The difference was found to be negligible; most of the technical solutions were already in place, and the vast majority of the program's requirements were within the administrative and process realms, not the technical realm. Furthermore, given Bahrain's centralized government data network, many technical solutions could be deployed at a central location, which reduced cost.

Challenge 4: How is this program going to succeed?

The Bahrain CIO set up a 1-year trial period with six government entities participating. During the trial, security project personnel met with government entities on a weekly to bi-weekly basis, constantly checking progress, tracking comments on Program forms and other documentation, and gauging the cyber security posture before and after implementation. This 'pilot' project proved immensely successfully, even though the target maturity level for most participating entities was the most basic level.

Implementation

The Basic "Maturity Roadmap" for each government entity includes the following specific action items:

- Conducting an assessment of each current operational area and its place on the capability maturity model scale.
- Coordinating with internal leaders to apply a risk-based approach to identifying Cyber Key Terrain (CKT).
- Establishing and evaluating the appropriate readiness level for each area of CKT.
- Identifying the steps necessary to move each area of CKT to the required level of security readiness with an implementation plan.
- Identifying the ongoing requirements to maintain the appropriate readiness levels.
- Establishing an audit system with reporting requirements to verify maintenance of standards, identify deviations, and implement necessary adjustments on an ongoing basis.
- Establishing the appropriate roles and responsibilities of each agency leader for CKT.
- Establishing the appropriate coordination mechanisms for information gathering and intelligence sharing.
- Implementing state of the art technology for threat detection appropriate to each identified risk to CKT.
- Assuring appropriate protections for privacy and human rights.
- Establishing the long-term plan for building and maintaining capacity.

The modular step-by-step design and not placing all groups in a single readiness track is intentional. There is a range of possible activities for each domain and these vary across each agency – this is the foundation of a risk-based approach to creating an adaptive defense.

Not every area within an agency needs the most advanced security. Identifying "security zones" or "CKT" is critical to identifying groups or assets that are worth defending or whose loss would be disruptive. The modular step-by-step design and not placing all groups in a single readiness track is intentional. There is a range of possible activities for each domain and these vary across each agency – this is the foundation of a risk-based approach to creating an adaptive defense.

How to Measure Value

Government entities enrolled within CTP would start an implementation based on the agreed implementation plan between the government entity and CIO. Government entities must also perform a quarterly self-assessment. The assessment includes a review of the agency status for maintaining the existing level of security readiness and requirements for an implementation plan to achieve the next level of security maturity. The objectives of the self-assessment are to ensure action has been taken on any existing level non-conformities and to monitor progress against implementation plan towards a more advanced security maturity requirements

Government entities are also required to conduct an annual external audit. The external audit may be carried out directly by the CIO, or by any suitably

qualified and CIO pre-approved third-party auditing firm. The purpose of the annual audit is to validate the self-assessment report, validate conformance to the achieved maturity level, identify any minor or major non-conformities, ensure actions were taken on previously identified minor and major non-conformities identified during self-assessment or external audits, and recommend or suspend maturity level based on audit finding

The CIO awards the maturity level certification after the 'External audit' process if the agency conforms to the criteria required by the maturity level by substantially attaining its requirements. Certification will remain valid as long as the entity conforms to the criteria of the Plan requirements pertaining to the respective maturity level. Certification may be suspended, downgraded, or revoked based on audit findings and the actions.

The Cyber Trust Programme effectively applies each core security domain at a level appropriate to the threats and risk posture of the organization and adjusts strategic decisions based on real-time, global, actionable intelligence coordinated by the CIO.

The CTP process can help create an increased understanding of existing capabilities and an accurate assessment of needs. This provides greater awareness of risks and improves the security readiness process. The development of an information security maturity model requires long-term planning and internal support. This will place Bahrain in a better position to detect and defend against sophisticated cyber security threats.

Leadership: Creating a Successful National Cybersecurity Programme

This Bahrain Program's success depended primarily on two key elements: Having cabinet-level support and having the right people on board.

A program such as CTP is designed to disrupt operations on a whole-of-government level, so it was nearly impossible to achieve this without the appropriate buy-in from senior government decision makers. When the Bahrain CIO suggested the CTP idea to Bahrain's Supreme Council of ICT, he initially proposed that the program be elective for government entities as he couldn't anticipate the reaction to radical changes. However, not only did the Supreme Council of ICT approve the proposal, they instructed the CIO to convert CTP to a *mandatory* program for all government entities to participate in, and to raise compliance reporting to the (higher) Bahrain Supreme Council.

Getting the right people on board, was achieved by the team in-house that was already eager to get the program started, and partially by having an open and inclusive approach in developing and testing the program. Also, by opening the CTP for input from the wider government community of IT personnel, the available body of knowledge increased substantially.

With these elements of the right people on board, a solid plan, and leadership support, the Bahrain Cyber Trust Programme had a strong foundation for achieving success.

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000.

The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.

The Kosciuszko Institute organizes European Cybersecurity Forum – CYBERSEC – the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe, and also publishes the European Cybersecurity Journal – a new specialised quarterly publication devoted to cybersecurity.

Office: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: ik@ik.org.pl

More on the European Cybersecurity Forum: http://cybersecforum.eu/

More on the European Cybersecurity Journal: http://cybersecforum.eu/en/about-ecj/