ISACABratislavaOC99results
7.6.2017/ Paul Wilkinson

Cybersecurity. It's all about attitude and behavior.

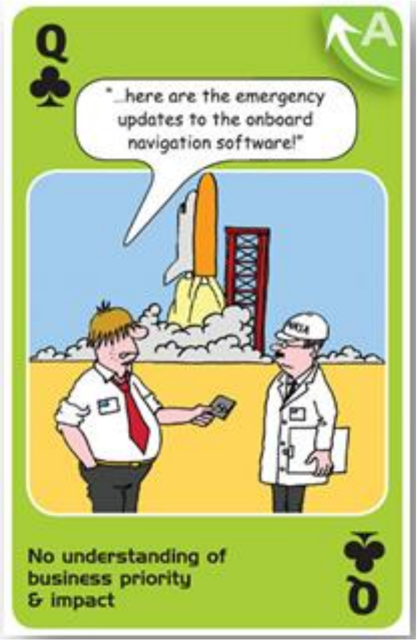
'Digital transformation represents the beginning of the most significant transformation in our lifetimes'. Michael Ganser Senior VP CISCO Central Europe.

Security however, is a barrier preventing many organizations from fully embracing the potential of digital transformation, and was named as one of the top 2 challenges by business executives. It is understandable why organizations are becoming increasingly concerned, as a 2016 FBI report suggested that Ransomware will be a $1 billion dollar industry next year.

This prediction seems to be frighteningly accurate. In recent weeks the World has been shocked by the global reach, scale and impact of this type of attack. An alarming growth is for Cyber criminals to target more the human 'behavioral' weaknesses in the system.

As highlighted in the ISACA guidance CSX (Cybersecurity Nexus) – "One of the most important root causes for successful attacks is human error on the part of the person or people being attacked" – behavior!

"….it's more than simply the behavior of those being attacked. Information Security has become an important element in the effective Governance of Enterprise IT", stressed Paul Wilkinson from GamingWorks in his closing keynote speech at the Isaca conference, adding that "Governance is more than simply gaining an auditors 'tick in the box'". Paul went on to quote the South African King IV report "Corporate Governance should be concerned with ethical leadership, attitude, mindset and behavior", which echoed the GamingWorks presentation which revealed that the same 'Attitude (mindset), Behavior, Culture' (ABC) worst practices have been chosen consistently for the last 15 years in workshops with more than 3000 organizations. The top ABC worst practice chosen being:


Q ♣
A
"...here are the emergency updates to the onboard navigation software!"
NASA
No understanding of business priority & impact
Q ♣

You can see how old the cartoon is. The IT person is holding a 'Floppy disk'!

Changing Attitudes and shaping new Behavior
GamingWorks conducted an Oceans99 Cybersecurity business simulation game at the ISACA Bratislava conference.
The goals of this workshop were to explore the 'Attitude, Behavior and Culture' aspects of Cybersecurity, and to show how the CSX (Cybersecurity Nexus) guidance gives sound guidance on addressing this.

Oceans99

In this business simulation game: "The owner of the Bank of Tokyo has decided to exhibit three world renowned objects. The 'Star of Africa', the 'Jewish Bride' and a 'Bugatti 59'. The challenge for the team is to bring the objects to Tokyo, on time, safely and securely, and to have them exhibited, however there are rumors that Oceans 99 a criminal organization wants to steal the objects… In the game the various stakeholders make use of Information systems for planning, for managing, for transporting, for monitoring the objects and for booking and selling tickets, there are many opportunities for Oceans99 to exploit vulnerabilities.

The team was given the tasks of designing a Security Policy, Performing a Risk assessment and developing a Strategy for investing in security counter measures. An observer was given the CSX COBIT 5 Model Behaviors in Cybersecurity and was tasked with making observations and giving feedback between game rounds.

What happened next?

'It's chaotic' said the Las Vegas car owner. The director of the Amsterdam Museum considered withdrawing his painting from the exhibition "I have no confidence that they have a clear policy'. The board stated to the CISO what they wanted then adopted a hands-off approach showing no 'accountability'. Cybersecurity policy was seen as an IT issue, not a business issue! The game facilitator, playing a potential investor with assets of $500 Billion asked the board for a presentation of their Policy, stating 'I want to hear the board vision on Cyber security'

When presenting the Policy the critical assets were seen as the physical objects and critical technology systems, and were not described in terms of 'Image' & 'Reputation', 'Critical data and information assets' that could damage reputation such as 'Credit card details' or 'Route maps' that the criminal organization Ocean99 could access and exploit. "I am doubtful about investing, this doesn't instill me with confidence" said the investor.

At the end of the game round we explored some CSX guidance that the team had ignored - COBIT 5 for Information Security Principles: The first principle being 'Focus on the business'. Ensure that Information security is integrated into essential Business processes.

We also explored the recommendations in a recent McKinsey report entitled 'Protecting your critical digital assets: Not all systems and data are created equal', which stated 'The idea that some assets are extraordinary – of critical importance to a company – must be at the heart of an effective strategy'. The team had failed to identify and agree the 'Critical information assets' that needed protecting.

These were the Key take away learning points from the Policy exercise:

- Lack of ownership and poor co-ordination of Policy definition. The Business was engaged for 1 minute, threw it over the wall to CISO and gave CISO no mandate to define a corporate wide Policy. Many recognized this level of Board commitment!
- The need for a structured approach and effective communication as to how the process would proceed.
- Lack of overall accountability. Some stakeholders try to pro-actively engage and show accountability, others wait to see what would be 'thrown over the wall'.
- The CISO should ensure 'Security needs' are embedded into the processes and behaviors of all Customer touch-points (e.g. in a real organization this could be Project management, Business Relationship Management, IT Service Management, Agile or DevOps teams) – ensuring that security is embedded both in business AND IT processes, roles and activities.
- Lack of a shared understanding of what the critical assets are, and what the business goals and drivers are.

ISACA Slovakia
Digital transformation
and it's implications to Information security
VÝROČNÁ MEDZINÁRODNÁ KONFERENCIA
1.-2.6.2017 / June 1st–2nd 2017
OCEAN's 99
Agreeing Critical Assets
Identifying Threats, Risks & Vulnerabilities with the Board
Investing in countermeasures

Considering the fact that the team were all certified security professionals we showed them the COBIT 5 'Model Behaviors in Cybersecurity' and stated that this is something that they 'should have been doing'! Perhaps more emphasis should be placed on these behavioral aspects in Cybersecurity certification. Below is a selection of some of the desired behaviors from CSX):

- All Users understand the defined priorities in Cybersecurity and how to apply them their personal and business IT environment
- All Users are aware of, and ideally actively involved in, defining cybersecurity principles and policies
- Security managers and Users share accountability for Cybersecurity. This includes business use, travelling and home use.
- Users have a clear view of their accountability and act responsibly.
- All Users are stakeholders in Cybersecurity, regardless of their hierarchical level within the enterprise.
- Executive managers act as end users and recognize the value of Cybersecurity. They actively participate in training and awareness activities
- Users are sufficiently aware of the risk, threats and vulnerabilities associated with attacks/breaches.

Paul revealed that one of the most critical enablers in COBIT 5.0 is the 'Culture, Ethics and Behavior' enabler, however the guidance has still not be produced. Paul made a case for the need for this in his blog and asked delegates to mail a call to action to Isaca for producing this guidance.

Risk exercise

The team then performed the risk exercise. They started following the guidance in the COBIT 5 'Model Behaviors in Cybersecurity'. The team got together and created a Risk Matrix. The CISO explained what Threats, Vulnerabilities and Risks meant. Each stakeholder was made responsible for defining risks from their business perspective.

The top 5 risks were then presented to the investor to show that the team had identified which key threats needed mitigating. These were all related the 'Cloud', 'Wifi', 'Tracking systems', 'Critical Laptops', 'Tags'.

"I am still not impressed" stated the investor. "In the keynote presentation It was revealed that 'one of the most important root causes for successful attacks is human error on the part of the person or people being attacked'….where is this in your Risk matrix and countermeasures"?

In the meantime the owner of the Amsterdam Museum had opened a Phishing mail and allowed Oceans99 to take over the tracking system. The team had fallen victim to the human error.

Other object owners had seen these phishing mails. Only one had reported an attack to IT support to register as an incident. This meant that 1 out of 5 security attacks was actually recorded – providing little ability for future risk assessments.

During reflection the team reflected once again on key learning points to take-away 'what was successful in this round that needs to be taken away'?

- A clearer picture of threats emerged when all stakeholders are engaged in the exercise, taking ownership for assessing risks to their business activities and information assets.
- The board must communicated their strategy, goals, priorities and gain commitment from all stakeholders (as opposed to the Policy exercise when they took a hands-off approach and showed little ‘ownership’).
- The CISO had given training and coaching to stakeholders helping them understand ‘Threats’, ‘Risks’, and ‘Vulnerabilities’.
- Not all have sufficient expertise to determine vulnerabilities and admitted this, as a result external services were budgeted: e.g. ‘stress test’, ‘integrity checks’.
- In the hectic of the moment the teams had reverted to behaviors they knew – ‘a Technology and systems’ focus on Risk. Ignoring ‘The people factor’.
- The team had no agreed or assigned priority mechanism for aligning Risks to the business drivers and priorities

After reflecting on what went well, what went wrong and revisiting the Policy and Risks (iterative improvements). The team made investments. One key investment was ‘Cybersecurity awareness training, - not generic – but based upon experiences gained, using organizational specific situations and examples of behavioral issues’. Helping address a recent statement from DarkReading: ‘The sorry state of Cyber security awareness training’

At the end of the session we explored Key end-of-day learning points. ‘What have you discovered, that you will now take away and do differently?

- Risk Management. More formalized Risk management, engage ALL stakeholders. Ensure that Risk Management in an ongoing exercise and uses ‘incident’ information. Ensure stakeholders take accountability for this.
- Improve awareness training, using organizational specific situations (e.g. from captured incidents and attacks) - for individuals answering the question ‘What does it mean to me’? Adding experiential exercises like this simulation, or practical assignments to let people see, feel and experience – in a SAFE environment. This helps create understanding, buy-in and commitment. (Attitude, Mindset, Behaviors).
- Policy and procedures: More formalized, defined processes and responsibilities for shaping the Security Policy and performing ongoing Risk management - to speed up the flow of decision making.
- Mutual awareness & Understanding: between Business and IT. Shared understanding of goals and priorities. The CISO can facilitate and enable this.
- External promotion (e.g. on Website, to demonstrate the corporate policy and show how we protect customers and help customers protect themselves).
- Demonstrate in order to build Trust and Credibility. Demonstrate an understanding of business goals, demonstrate adherence to policy, demonstrate value and impact of actions, demonstrate an understanding of the business impact of security.
- Incident management and responses: The importance of the Help Desk and Incident management for accurate recording, classification and analysis of security related incidents. The important Role that Problem Management can play working with the CISO. Ensuring this feeds into Risk management.
- Getting the big Picture. Too often we are caught up in the daily operations and technical details. We need to understand how, what we do impacts business strategy and goals. We are not protecting systems, we are protecting business value. This game allowed us to see the need to manage it from end-to-end.
- More face-to-face awareness sessions. To discuss, share, explore and confirm understanding and commitment.
- The need for executive level management commitment & support.

This was a critical point. In the beginning the team members confirmed lack of ownership and governance from board members. In round 2 the board was committed and took ownership. What had the team done to get this?

‘Showed an understanding of business drivers and impact on business value generation as well as explaining risks in term of business impact and loss of value, damaged reputation. Demonstrating to the business we are thinking in business terms and not technology and systems terms.

- ‘Persuasion’. CISOs often do not have the mandate and authority to change attitudes, mindsets and behavior. They must use the power of ‘understanding’ and ‘persuasion’. Develop ‘Communication’ skills.
- Leverage the experiences of the past. Start performing ‘Retrospectives’, looking at incidents, attacks, risks. What worked well, what can be improved, what did we learn?

‘This was a powerful example of effective awareness training that also gave us items to take away and apply’. Said one delegate, showing a change in attitude and a commitment to behavior change.

The workshop was also a good way of addressing COBIT requirement: EDM01.02 Direct the governance system – ‘Obtain senior management commitment to information security and Information risk management’. In the game the Board had turned from one displaying ‘no ownership’, to one that was actively engaged. Perhaps it’s time to play a game with your executive leadership team and board.