CYJAX

Digital Intelligence
Securing the Future

Eight Security Leadership Principles

PRIVATE & CONFIDENTIAL

Date: 07/04/2021

About Cyjax

We aim to safeguard your data and secure your future. Our mission is to be the preeminent supplier of digital threat intelligence for enterprises, SMEs and governments around the world. Established in 2012, Cyjax has built a reputation for producing world-class digital threat intelligence across a broad range of areas. The company has developed its own innovative technology from the ground up. This, combined with years of experience in the intelligence community, has led to Cyjax evolving into a class-leading digital security and intelligence company.

Eight Security Leadership Principles:

"Being prepared for the worst of times will let you enjoy the best of times." - Phat_Hobbit

I've recently been engaged in a sudden and in-depth retrospective analysis of how, in 2017, I could have changed the fortunes of a five-billion-dollar company and set the wheels in motion to change the culture of the organisation to embrace security. The reason a culture change is required is that corporate security and product security cannot exist as separate entities. They are conjoined and inter-dependent.

What follows is largely based on my observations as a "security" person over the last 20 or so years with experiences to share from work in small, medium, and enterprise organisations. I'm not an expert security strategist, tactician, practitioner or analyst. I have strengths and weaknesses like everyone else inside the security community and outside - on occasion I get things wrong too.

So, what am I actually good at, and why do some people view me as valuable - why should you pay attention to what I have to say? I'm good at learning, I'm really good at communicating and I'm good at helping others adopt and improve organisational security through an intelligence-led approach. These security leadership principles have been brewing since I had the chance to "invent" them in 2017 and failed to make enough of an impression to make an impact. My advice is to not make the same mistake as a five-billion-dollar company did in 2017.

Also, one more piece of advice. Don't agree with everything I have to say and don't accept it as some security "Gospel". Debate the practicality, application, execution and validity of the ideas with rigour and scrutiny. Within the confines of these principles, I hope the value of them is self-evident but if that value is obscured in better times, you can find me in the pub, I will buy you a pint and you can tell me "just how far on the side of wrong I am."

1 Achieve personal and professional security competence

"Being secure is not a choice, it's a lifestyle" - Phat_Hobbit

Looking back at my security career of some 25+ years, the conclusion I've come to about the state of organisational security is not because I've now been over-exposed or demoralised by a never-ending stream of Instagram and Twitter motivational quotes. It is a conclusion drawn from bearing witness to the repeated failure of organisations to protect their infrastructure and systems, having their customer data pillaged and most tragically a failure to learn from organisations which have succumbed to the ravages of cybercriminal and advanced persistent threat (APT) groups.

Note this first Principle of Security Leadership is not about developing expertise or world-class skills. This principle is about developing an understanding of both the concepts and controls required for delivery of organisational security - and not as a "zero sum" answer to the impossible question of "is our organisation secure: yes, or no?". Because organisations and the people of the organisation are dynamic, security leadership is also required to be forward leaning and anticipatory of the organisation's needs. Delivery can be delegated to technical experts, but the strategy needs to be rooted in a competent understanding of risk, threats and appropriate controls against these hostile elements.

Organisational security has nearly always been defined as "Something, Something, People, Process & Technology". From a control perspective this may be true but even security programs that embrace employee awareness, have accurate process documentation and the latest and greatest cybersecurity solutions are successfully attacked by sophisticated and at times unsophisticated actors. Why? The answer is relatively simple: a lack of empowerment, strength of character, and gravitas of action. In short - security leadership to unify and align the people, processes and technology to support the mission of organisational security.

Without security leadership the dynamic nature of organisations slowly - like shifting tectonic plates - move the people, the processes, and the technology out of alignment with the mission. In the physical world this action causes lava to pour fourth; in the cyber world these silos are points of weaknesses to be targeted by malicious actors. In a successful breach, your organisation's data pours forth, much like lava.

One of the key components of competence is maintaining situational awareness of both internal events and external events which may impact your organisation. It's disheartening to see organisations fail to take security seriously, time and time again, even with ample warning from private industry and government agencies, and having to subsequently beg forgiveness from their customers and employees.

2 Embrace personal and professional security improvement

"If you don't know where your security is at, it is very hard to get your security improved." - Phat_Hobbit

At some point, despite the efforts of you and your team (if you are fortunate enough to have a team), security at your organisation is going to fail. It is both inevitable and something that can be prepared for. If organisations are dynamic so, then, are the adversaries who may have an advantage of speed and agility over your own organisation. The key takeaway from this point is opportunities for personal and professional security improvement are readily available.

So, what is the key ingredient here? Embrace those third party risk assessments, pen tests and "red team" and/or tabletop exercises - these are the vital components. It is nearly impossible to understand areas to improve security in your organisation without a benchmark against which to measure the improvement. The vital ground is not necessarily straight-up improvement but setting the priority of incremental efforts. Logic dictates that priority needs to be aligned to organisational risk, be highly effective and of low cost. The time-honoured tradition of "doing the most with the least."

This is not an impossible exercise. There is a multitude of free tools and best practice guides to help with this. But as a security leader you have to rein in your ego and personal feelings, as mistakes will be found by talented individuals with more knowledge and more experience than you. From a philosophical perspective, embrace the good revelations and improve the poor revelations. Accepting that you may not know everything is a key part of understanding when you may need to go to your network to ask questions. And seeking outside advice – asking questions – is critical.

Personal and professional security improvement is not about executing a ‘To Do’ list. Open your mind to the possibility of creative problem solving by enlisting the aid of those with more knowledge: both inside and outside your organisation. Remember if the adversary is dynamic at offensive operations, you and your team need to be dynamic in defensive operations. This brings us again to situational awareness: you need to know how malicious actors will strike your organisation and prepare accordingly. The breach data suggests that 90% of cyberattacks start with a phishing email.

3 Accept personal responsibility for security

"I told the OVH Intern to check disaster recovery capability, what happened next was umm...unexpected" - Phat_hobbit

This is the essence of security leadership. In good times and bad, accepting responsibility for events that happen on your watch is key. Mistakes will happen; security breaches will occur; but it is how a leader accepts responsibility that defines them - with grace when good and humbleness when poor. If a security leader has fully embraced personal and professional security improvement (number 2), taking responsibility is natural.

The danger of not fully embracing personal responsibility is when this acceptance is avoided or not genuine. Nothing will endanger your credibility as a security leader more than "blaming an intern" or characterising a plan for improved security controls as anything less than an admission that security was inadequate to begin with. Customers, employees, and shareholders are not stupid, and they will see through the charade.

This is especially true when events conspire to draw the scrutiny of the media upon an organisation's actions and statements as a security event unfolds. It's fair to say that there is a place for Public Relations and spin, and that these are to be expected to some degree in the description of an event that reflects poorly on your organisation. But where PR and spin turn into scapegoating, leaving mouths agape and causing outrage at the blatant lack of responsibility being taken, the leadership in that organisation may suffer irreparable damage to its credibility. Anything further is defaulted to extreme scrutiny and mistrust.

There is some hypocrisy in accepting personal responsibility for everything. We live in a society where feedback and even criticism is not generally publicly administered, yet positive accolades are generally given publicly. As previously mentioned, security success is generally due to the alignment of people, process and technology, and is an organisational mission. Thus, humble acceptance is required on the part of the security leader as a "team effort" with "good tools" and "clear processes". In security there is rarely an "intern zero" to blame when a security event happens.

4 Set a personal example of being secure

"When it comes to cyber security, one person in your organisation can make a difference." - Phat_Hobbit

Rules and policies in your organisation are in place to prevent unauthorised disclosure of sensitive information and information that could be leveraged for malicious advantage. The rules and policies are generally aligned to the best industry practices and try to balance the need to collaborate and provide value to the organization, while at the same time preventing social engineering, physical and cyber-based attacks.

The organisational guidance does not disappear or become invalidated as soon as the clock strikes 5:00pm, or over weekends and holidays. Perhaps the single most important personal example you can set is adhering to the polices of your organisation especially if you are regarded as an influencer, manager or executive – someone others are likely to look up to.

Given that slightly more than 2/3 of our waking hours are outside of traditional working hours there is opportunity to practice what you preach in your personal life and allow those good security habits to inform good security behaviours. One way to develop this mind set is to think of access to a collection of "data" as access to a pile of "cash".

Following significant fraud, banks in the EU/UK have, as a result of legislation called SCA, mandated multi-factor authentication to protect users from fraudulent activity - to protect your "cash". So, in your organisation if you can access hundreds if not thousands of potential sensitive documents and data over a Remote Desktop Server that is only protected by a user ID and password: does that seem right?

One of the most effective ways to combat cybercrime and be personally secure is to turn on MFA for all your personal accounts and help others turn on MFA. Be a champion on MFA in your personal life, if others ask you about security and as a security leader work to get access to your organisation’s "cash" protected by MFA.

5 Ensure everyone knows the meaning and intent of the security program

"If you don't understand the "why" of security program then the "who","what,"where","when" & "how" will not matter" - Phat_hobbit

One of the single most destructive phrases in the English language is "I'm not technical". This phrase is far too often used to justify a position of disengagement when chances are technology, and a failure to use it safely, is capable of significantly impacting your life both at work and at home.

"Looking both ways before crossing the street" was a phrase used to teach children to be careful. In a world where those roads are copper wires, and data breaches can have astonishing financial and even physical consequences for an organisation, it's important to concentrate on "why" personal and professional security is critical to the organisation.

The security industry is partly to blame for complicating matters, adding esoteric phrases such as "threat/risk model" & "Intelligence Requirement", and other obfuscated terms. The reality of all these overly complicated terms means that most people who are not versed in esoteric security language are left in the dark. The "people" silo of security is easily fixed by concise answers to four questions:

1) How does the organisation receive money for its product and/or services?

2) How does the organisation send money to its employees, contractors, and supply chain partners?

3) What is the unique value proposition(s) of the organization?

4) How is the unique value proposition(s) safeguarded?

Questions 1 & 2 are easily solved with an infographic or a picture showing the "flow" of revenue and expenses and what systems are required for those flows. It's a simple exercise and will help those "non-technical employees" understand why a security program is important to safeguard the "flow".

You can even identify some of the security controls in place to assist in that mission. Any incident that jeopardises the confidentiality, integrity or availability of the systems involved in "the flow" would be considered serious.

Questions 3 & 4 are critical in providing the "why" and encouraging buy-in from all employees. The security program is in place to "protect the money and protect that which makes the money". From an uncomplicated perspective this is the "vital" ground of the security program and if the answers to the four questions are elusive among the staff, failure of the organisation's security is highly likely.

"Complexity is the enemy of security." - Bruce Schneier, 1999 Truer words may have never been said. A security leader has to simplify the complexity in the organisation among all three silos: people, process and technology. A simple message is both easily understood and remembered. A simple process is less likely to deviate or fail. And simple technology is easier to implement and maintain.

6 Embrace security improvement opportunities

“If you don’t know it exists, how can you secure it?”- Phat_Hobbit

Security improvement opportunities will always be found around you, both personally and professionally. The art of security leadership is found in delivering those improvements with minimal investment of time, money and effort. The majority of my personal successes in securing organizations large and small came from working with managers, directors, teams and departments far outside security and information technology.

I call these opportunities ‘organizational security choke points’, where minor changes to processes outside of one’s technology-focused departments can drive massive security improvements downstream in the organization. Marketing, Procurement, Project Management, Sales, Governance and Risk, Legal, QA & Development and Accounting departments are valuable potential allies to engage with when trying to improve organizational security.

Organizations today are dynamic, with mergers, acquisitions and divestments having a tremendous impact on what is exposed to the internet – this is frequently called “the organization’s external attack surface”. One of the largest disconnects with organizations is that the IT department may know what the organization has exposed but it may not know why it is exposed and who in the organization is responsible for it. I spent nearly a year on a project at a billion-dollar financial services company just getting an understanding of the external attack surface.

Whilst I had a good tool and an excellent resource for this effort, tracking down the organization owner of a system was deeply problematic until I enlisted the aid of the accounting and marketing departments. As it turns out, we discovered numerous development environments and systems that should not be exposed as well. Nearly 60% of the over 2,000 domains were no longer required due to divestments, consolidations, and straight up abandonment.

The project saved roughly half a million dollars over the next two years and working with the procurement team we set up a “new domain or domain renewal registration approval process” to ensure the security team had visibility of any new system that needed to be exposed or an existing system that was exposed and needed to remain so. The external attack surface was reduced further by moving systems that did not need external exposure inside the corporate perimeter or accessible only via VPN. This information was then used to increase the effectiveness of the Vulnerability Management program to target exposed systems on a priority basis.

Security leadership is about applying a “root cause analysis” to the earliest stage of a problem – How did this security problem happen? – and then applying a cost-effective solution to that early stage – How can we prevent this security problem from happening again?

7 Make sound and timely security decisions

“Security vision without security resources is hallucination” - Phat_Hobbit

In the early part of this paper, I mentioned one of the things I’m good at is improving organisational security through an intelligence-led approach. The creation of intelligence to make sound and timely security decisions is about applying discipline and a methodology called the intelligence life cycle to information to create recommendations which are accurate, timely and actionable.

*The **intelligence lifecycle** is a **process** first developed by the CIA, following **five steps**: direction, collection, processing, analysis and production, and dissemination. The completion of a **cycle** is followed by feedback and assessment of the last **cycle's** success or failure, which is then iterated upon.*

It’s out of scope to turn this whitepaper and lecture into a lesson on intelligence analysis but suffice it to say that these five steps of turning raw information into something useful and learning from failure align closely to the overall security leadership principles I’ve discussed. You don’t have to be a government or military trained analyst to understand how this works – in a lot of cases it’s instinctual to make conclusions based on evidence and not wild fantasy.

In fact, to not over complicate things with a CIA five step process there are two philosophical rules you can apply to situations that will get you very close to sound decision-making. You are probably already familiar with them:

Hanlon's razor: "never attribute to malice that which is adequately explained by stupidity or an innocent mistake."

Ockham's razor: “There exists two explanations for an occurrence. The more assumptions you have to make, the more unlikely the explanation is.”

Sound security decision making is rooted in evidence and the ability to draw a logical line between the observed current state and desired future state. The critical part of security decision making is found in iteration and analysis of making the “right call” or the “better call”. It is best to not think in terms of right and wrong, only sub-optimal and optimal. "Wrong" has the perception of being negative, emotionally charged, and tainted with accusation.

In terms of understanding the importance of a timely decision, perhaps an allegory will do. The deer which freezes in the headlights of an oncoming car usually has a sub-optimal outcome. The same is true of security. Although doing nothing may be a legitimate choice under some security circumstances, it is generally harder to justify taking "no action" then applying logical thought and taking an "action" or "actions" – even if the "action" or "actions" were ~~wrong~~ I mean sub-optimal.

One last philosophy to apply to security leadership is the concept I like to call Schrodinger's Security Cat. "You can't know if your security has been breached until you have evidence your security has been breached." Thus, just like the cat in the box being both alive or dead, your organization can be secure and breached at the very same moment.

"The art of security leadership is simply to make a reasonable decision with a limited amount of evidence in a very short period of time." – Phat_hobbit

8 Never ignore a security incident, inform your supervisor and/or security operations

"Removal of the evidence of a security problem is great way to claim a security problem never existed to begin with." – Phat_Hobbit

One of my assignments in the Canadian Forces junior officer training program, Common Army Phase Training, was to write about what I thought was one of the best leadership characteristics to demonstrate. Being a bit of a politically left- leaning Military Police Platoon Commander, I picked "compassion"- hilarity ensued and by hilarity, I mean a lot of shouting (instructors) and running (my course mates). Since in this paper and lecture I have been talking about iteration and opportunities for improvement as a security leader, I will now revise my thoughts on what constitutes the best leadership characteristic to 'being magnanimous'.

Magnanimous comes from Latin magnus "great" and animus "soul," so it literally describes someone who is big-hearted. A person can show that over-sized spirit by being noble or brave, or by easily forgiving others and not showing resentment. This is the most important – saving the best take away from all this for the last – of all of the security leadership principles I've put forward.

You cannot see that which is invisible and the organization in the midst of a security event is a lot like paramedics arriving at an accident scene. It's likely they are arriving to deal with someone or some people who are having the worst day of their lives. If security and IT are perceived as unapproachable, vindictive and focused on blaming and shaming those responsible – even tangentially for a security incident you have completely failed to unite the people, process & technology to the common organizational security mission. A lot of things – potentially very bad things – will happen, and your security and IT teams will be the last to know – if they even find out at all.

It’s critical to gather data and information to inform appropriate decision making. Without that intelligence there is a danger of overreacting or underreacting to a security event. You will gain far more actionable intelligence if your employees are comfortable approaching you or your team with a security question or security concern that is always an opportunity for security improvement – a golden moment. Security leadership is about being outside the comfort zone of just relying on process or technology. A security leader must engage in the security conversation with everyone in your organization.

“Cybersecurity leadership is about what you don’t know, who you know that might know and how you grow from each security success or failure.” – Phat_Hobbit