A Model For Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor, and Leadership

WILLIAM PELGRIN
Center for Internet Security

Abstract. Virtually every aspect of modern life is shaped by advancements in technology. While there are undeniable benefits to this ubiquitous use of technology and the Internet, we must also understand the security risks that come with them and take appropriate measures for preparedness. The challenges faced by government, industry, and academia continues to grow in volume and complexity as cyber security threats constantly evolve. The need to ensure that cyber security best practices are ingrained in everyone’s behavior and continue to be an essential component of business operations has never been greater. Good cyber security is built on layers—a defense in depth strategy. A critical component of this strategy is to improve our cyber hygiene through positive change in behavior. The paper explores innovative ways to influence long lasting outcomes in three areas: cyber security strategy, human factor, and leadership.

Keywords. Baseline assessment, controls, cyber security strategy, experiential learning, human factor, information sharing, leadership, metrics, prioritization.

Introduction

Cyber security is now part of the mainstream consciousness. The vast majority of us have not just heard or read about cyber threats but, sadly, have also been a victim of a cyber incident. These incidents include credit card compromises, data breaches, scams, phishing, identity theft—the volume is overwhelming. Being a cyber victim is almost a rite of passage. No single segment of society is immune—individuals, corporations, governments, and nations are all under constant attack from cyber criminals. Cyber criminals encompass a diverse demographic as well—teens, hacktivists, hackers, nation states, and terrorists.

Cyber security threats know no geographic or demographic boundaries; public and private sector organizations alike face the same challenges. Potential impacts of cyber-related incidents include the disruption of essential services and critical operations or worse, that of property and loss of life. Cyber security can seem overwhelming to many, especially in light of a depressed global economy in which resources to defend against threats are scarce. It is difficult to know what to do or where to begin, especially for those lacking experience or resources. Often it is the start that stops most of us.

With our increased awareness about cyber risks, one would have thought that by 2013 everyone would be employing good cyber hygiene in order to protect themselves.
Unfortunately, we are not. Our behaviors have not changed significantly in light of the current threats. Internal processes have not embraced cyber security as an integral part of the business function. Too often technology is seen as the solution versus a tool that can be used to more securely protect information assets.

Many of the issues and concerns about cyber security threats and mitigation strategies that were being discussed ten years ago still hold true today. Too many organizations do not require strong passwords, users are insufficiently trained, systems are not patched, and users are still not cautious about clicking on links. These basic minimum-security layers, which would dramatically improve our cyber security environment, have not been universally adopted.

Approaching cyber security in a tactical, rather than strategic, manner is essential to effectively addressing these challenges. The general tendency is to discuss, analyze, and debate the same security issues repeatedly, without actually coming up with actionable measures. These behaviors have to change. Good cyber security practices must be as second nature as buckling a seat belt. Although 100% security cannot be attained, promoting positive behavioral changes minimizes cyber risks.

The need to ensure that cyber security is ingrained in users’ behaviors and continues to be an essential component of operations has never been greater. Moving toward a more secure posture, however, remains difficult due to an ever-changing threat landscape. Therefore, organizations need to perform constant monitoring and assessments to answer the question ‘Is my organization more secure today than it was yesterday?’

Effective metrics are necessary to inform decisions about good cyber security practices and ultimately to create a more secure environment. Measurements require first and foremost the establishment of a trusted environment in which to capture and assess metrics. Building a culture in which people can safely and accurately evaluate their organization’s network is necessary. The status of an organization’s network cannot be effectively measured, nor can progress be attained, if employees fear that an accurate picture of its security posture may lead to criticism, or worse. Creating this new culture starts with the principle that the assessment process cannot be about who to blame, but rather must identify what gaps exists in the system and what a roadmap to achieve an improved security posture should look like. Metrics are essential tools for organizations. Traditionally, metrics have been used to measure past performance (i.e., did the organization achieve what it planned to achieve? How well did the organization perform?). While this is one method of measuring success, it is by nature retrospective.

Metrics can also be used prospectively in order to promote positive change. The ability to affect decisions and behavior has a long lasting positive impact on improving an organization’s cyber security posture. As stated by Douglas Hubbard in *How to Measure Everything: Finding the Value of ‘Intangibles’ in Business*:

> If a measurement matters at all, it is because it must have some conceivable effect on decisions and behavior. If we can't identify a decision that could be affected by a proposed measurement and how it could change those decisions, then the measurement simply has no value.[1]

The paper highlights innovative ways to use metrics to change behavior in order to improve long lasting outcomes in three areas: cyber security strategy, human factors, and leadership.
1. Cyber Security Strategy

The ability to secure critical infrastructure from cyber attacks begins with a strategy. An organization typically spends a significant amount of time planning, researching, discussing, and designing strategies before choosing one. This does not diminish the value of planning—it is still an important process—but the tendency to over-plan may reduce its effectiveness. Indeed, by the time a plan is implemented, the infrastructure and threats may have already changed, rendering the chosen strategy insufficient to address the ever-changing landscape.

An effective strategy needs to be focused on deliverables by taking tangible steps toward a common approach to improve the cyber security posture. Getting down to business means knowing what those steps are and carrying them out.

Many good cyber security strategies already exist. Organizations need to identify the one(s) that works best for their environment and implement them. A good strategy must be realistic and implementable. Incremental adjustments to its complexity can provide achievable and measurable outcomes.

1.1. A Case Study on Developing a Cyber Security Strategy

A chief security officer for a large and diverse state government with more than 60 agencies and nearly 200,000 employees implemented a state-wide cyber security strategy across all agencies, using International Organization for Standardization (ISO) controls to increase the security posture of the state. In order to facilitate the successful implementation of the strategy, the controls were categorized into four levels of criticality so that agencies could incrementally address each level. Level 1 represented critical defenses; Level 2 focused on defensive readiness; Level 3 encompassed defensive planning; and Level 4 addressed security training and awareness. Compulsory timeframes were established for the implementation of Level 1 policy requirements, due to the nature of the items in this category. Implementation of Levels 2-4 was completed in phases. This approach improved the overall state security posture and is now being leveraged at a national level.

1.2. Recommendations on Leveraging Existing Cyber Security Strategies

Long-term plans must be flexible to address the ever-changing threat landscape. They should also focus on one to three year deliverables. These deliverables should be implemented and adjusted as needed. The strategies below can serve as a launching pad for any organization to improve its overall security posture.

Existing organization and national guides already offer actionable measures that can facilitate the broader use and application of a technology or a process to promote security. In particular, the Australian Government developed a document entitled ‘Strategies to Mitigate Targeted Cyber Intrusions’[2] and indicated that at least 85% of targeted cyber intrusions could be prevented by following four mitigation strategies:

- Use application whitelisting to help prevent malicious software and other unapproved programs from running.
- Patch applications such as PDF readers, Microsoft Office, Java, Flash Player and web browsers.
- Patch operating system vulnerabilities.
• Minimize the number of users with administrative privileges.

Of the four strategies above, the last three can be implemented in a relatively short time.

There are a few additional measures that can be implemented along with the previous ones, and are derived from the ‘Critical Security Controls’ strategy published by the SANS Institute:[3]
• Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers;
• Secure configurations for network devices such as firewalls, routers, and switches; and
• Security skills assessment and appropriate training to fill gaps.

2. Baseline Assessment and Prioritization

Long term plans must be focused on deliverables. The first deliverable of any good cyber security strategy should be an inventory of critical infrastructure assets or a baseline assessment. More often that not, an organization does not know what the composition of its enterprise is because new technologies, applications, and products are layered onto existing systems. If an organization does not know its assets, it cannot protect them.

In many circumstances, enterprise network administrators are not fully aware of what assets (service instances on network hosts) they have nor how these assets depend on and interact with one another. Therefore, administrators lack understanding of the roles network assets play towards supporting the missions of the enterprise. Consequently, administrators are unable to identify which assets are most critical and whether or not any resiliency is present (e.g., load balancing or failover) to protect those assets in the face of failures or attacks. Therefore, network administrators do not always know how best to proceed if an asset or network failure occurs, and security teams are unaware of which assets are in greatest need of security protection and monitoring.[4]

A complete inventory that is updated frequently is thus essential to knowing what comprises an organization’s critical services and assets, and knowing the information security and other controls that are in place to protect them. Once the inventory is completed, it is possible to determine the importance and dependencies of specific critical services and assets, their vulnerabilities, and the potential threats they face. An organization can then prioritize a list of controls that would have the greatest impact in improving the risk posture against those threats.

In short, dividing the tasks into prioritized deliverables should be the starting point of any effective strategy. Similar to how a hospital prioritizes its emergency response by triaging patients and treating the most serious cases first, cyber security must be handled similarly. Although this approach may seem elementary and obvious, many organizations do not employ it at all. A divide-and-conquer approach facilitates an effective strategy and builds a sense of accomplishment that can be easily quantified.
2.1. A Case Study on Baseline Controls

The Center for Internet Security (CIS), an international not-for-profit organization, recently handled a case involving multiple state and local governments in which the failure to inventory systems and prioritize patch management—a baseline policy—had a significant impact on their networks. Attackers were able to exploit unpatched vulnerabilities in twenty-two systems, gaining a foothold into various networks. At least one incident resulted in the compromise of an entire network, including domain controllers. Some systems were compromised for up to eight months after a patch had already been released. In each of these instances, a regular patching schedule would have improved the security posture as well as avoided the costs associated with remediation.

2.2. Recommendations on Baseline Assessments

In order to develop a comprehensive approach to information security, the first step must be to inventory critical infrastructure assets. The second step should be to use assessments and scans to identify the vulnerabilities with the greatest risk, and start addressing those first. An organization that fails to fix the most urgent vulnerabilities preemptively will still have to address them after a breach has occurred and incur even greater costs for remediation.

2.3. A Case Study on the Use of Metrics to Assess Progress

A large state implemented a report card system to measure and rate progress against common standards. This was a valuable component of its cyber security program. Each year, report cards were issued to all agency executives during a cyber threat brief, along with a review of the results from the year’s compliance activities. Metrics were compiled using visual graphs representing the various areas of the policy with the relative compliance percentages for each agency. Report cards were issued to each agency measuring its yearly progress, and metrics were provided to show where each agency stood in its progress relative to all other agencies and the statewide average. These report cards were not issued as punitive measures and were explicitly drafted in such a way that no agency would be blamed for not meeting a specific deliverable. Many factors were taken into account to rate an agency’s compliance with the standards. The focus was clearly placed on positive recognition where objectives had been met, on identifying gaps in compliance to the policy, and providing recommendations on how to close those gaps. The creation of this safe environment resulted in the participation of all agencies.

A certificate of excellence, signed by the Governor, was then issued to each agency that achieved overall policy compliance during an annual executive briefing for all agency commissioners. This recognition spurred healthy competition among the agencies and improved the overall state security posture.

Strengthening an organization’s cyber security posture, however, entails much more than getting a grade once a year and filing a report away on a shelf. This is an ongoing process that requires executives and security staff to work together to review progress and have candid discussions to identify issues and solutions. In the example above, every agency came into substantial compliance within a short time. The report card allowed agencies to measure their progress against security standards, enabled
them to track compliance over a period of time, and helped them rate their progress relative to their peers.

2.4. Recommendations on Measuring Progress

The following recommendations will help organizations conduct a baseline assessment, track trends and patterns, measure progress, and encourage compliance:

- **Establish concrete, measurable, and attainable metrics.**
- **Implement an incremental approach toward a more secure cyber posture.**
- **Create a report card process to encourage and track compliance.**
- **Compare results through the report card process across different organizations and reward success through recognition of achievements. This metrics methodology has proved itself as a motivator and healthy competition that encourages organizations to improve faster.**
- **Use metric questions, such as those found in the National Cyber Security Review (NCSR).**[5]

3. Timely and Actionable Information

There has been much talk about the importance of information sharing. The end state of information sharing, though, is not just the sharing itself. Information shared must be both timely and actionable. Out-dated, non-actionable information is unhelpful. All too often information is not released until every last detail is checked and rechecked. Although this is important to avoid overlooking important details or misinterpreting significant factors, perfection is the enemy of the good. It is critical to disseminate credible information as soon as possible. Information can always be qualified with a disclaimer, indicating that what is being shared is the preliminary or best information at the time of distribution. Threat actors will most likely already have all the information anyway. Delaying distribution will only withhold it from those who need it most.

3.1. A Case Study on Timely and Actionable Information Sharing

During a recent incident handled by CIS, timely and actionable intelligence had a significant positive impact in the overall response. An advanced persistent threat (APT) group targeted twelve critical infrastructure entities via a phishing email campaign (Sykipot malware). CIS immediately contacted those twelve entities and, after further analysis, identified what is believed to be the source from which the actors obtained the addresses—a publicly posted document containing hundreds of email addresses of individuals working in these critical infrastructure organizations across the country. CIS notified all the organizations and shared the indicators with the federal, state, and local governments. A number of the critical infrastructure entities reported back to CIS that they had identified the attack using the indicators shared via CIS bulletins and remediated the potential incident before significant damage occurred.

3.2. Recommendations for Timely and Actionable Information Sharing

The following are basic recommendations to guide effective information sharing practices:
• Ensure that the information being shared has real value and is not just a recompilation of something else.
• Ensure that analysis and action steps are tailored to specific audiences. Gearing products specifically to the intended audience will greatly enhance their value.
• Develop key partnerships. Public-private partnerships, as well as collaborations between civil and law enforcement sectors, must be established in advance and constantly reinforced. Knowing whom to call when there is a crisis is half the battle.
• Start to identify gaps in the organization’s contacts and then immediately develop working relationships with those who will be critical in a crisis.
• Be willing to give more than you get. You can’t break down barriers if you are territorial yourself.

4. The Human Factor

User behaviors can have a significant impact on the security of an organization’s environment. Symantec’s 2013 Internet Security Report stated that two out of the top three causes of data breaches in 2012 were attributable to human error (accidental disclosure, theft or loss of equipment).[6]

It would be a mistake to assume that every employee understands his or her individual responsibility for securing cyberspace. A sizable percentage of the workforce does not believe that they are responsible for the security of their organizations’ networks, and many of them may have not received appropriate cyber security training. Addressing the human factor is a critical defense strategy for improving an organization’s security posture.

Many of the recent high profile breaches, in which millions of records have been impacted, were the result of human error. In one case, for example, the breach was due to an employee falling prey to a phishing scam and clicking on a link in a malicious email. The ramifications were magnified by the use of weak passwords and unencrypted data.[7] In another case, an employee clicked on a malicious link in an email that had already been caught by the company’s spam filter. Thus, the individual made a number of bad decisions, from retrieving a suspicious email out of the spam folder to clicking on an unknown link in that email.[8]

Understanding how to incentivize cyber hygiene and promote good behavior begins with the recognition that all actions have consequences. In the cyber security arena, one rarely sees a tangible and direct correlation between actions and their consequences. Only in the movies does clicking on a malicious link result in the computer screen going black and the hacker’s face appearing right after. In the real world, nothing immediately blows up, melts, or looks different after you click on untrusted links, insert a thumb drive containing malicious code, or open a bad attachment. Trying to change unsafe behaviors is difficult because there are no immediate obvious negative consequences.

An effective measure to significantly improve user behavior is to employ a more experience-based approach in which individuals experience the lesson in a tactile way.
A major exercise was able to test this tactile-based learning experience through a large-scale mock phishing attack involving 10,000 employees across multiple agencies. With the consent of the agencies’ commissioners, two separate emails were sent to employees enticing them to divulge passwords on a linked website. The objectives were to assess communications and establish whether they positively influenced desired behaviors – specifically whether written directives that clearly identify the problem, discuss the risk and specify appropriate action, have any meaningful impact on behavior.

The exercise was conducted in three stages:

- **Phase 1**: An advisory bulletin was emailed to employees from each agency’s chief informing them about phishing scams – what they are, how to avoid them, and in particular why it is critical not to reveal sensitive information such as passwords.
- **Phase 2**: Approximately two weeks later, the phishing exercise was launched. This consisted of an email sent to the same set of employees, appearing to come from the agency’s information security officer, and asking them to enter their user identification and password into a new ‘password checker’ tool. If the employee entered his or her user ID and password, the exercise would end and a message would appear informing the employee that this was a phishing exercise and, had it been real, they would have just been hacked. Too many employees fell for the scam. Those employees immediately received remedial training and a quiz to help them recognize a phishing scam attack.
- **Phase 3**: A month later, another phishing exercise was launched to the same set of employees to see if the tactile approach made a difference in their behavior. The second phishing email came from a bogus department in their agency requesting the employees to click on a link and complete a survey. The metric consisted of identifying: who fell prey to the scams; did they already fall prey to the first one; did they learn anything and do better on the second exercise?

The number of people who fell prey to the second phishing scam decreased by nearly 50%. When employees were surveyed as to why they fell for the phishing scam, they indicated that they did not realize they were engaging in inappropriate behavior, even though they had read the advisory before the exercise was launched. Therefore they needed to have that tactile experience to understand and see the relationship between bad behaviors and falling prey to a scam in order to change to a positive behavior.

Other phishing exercises, both in the public and private sectors, have been conducted with similar results. As part of these exercises, information about positive behaviors in cyberspace was clearly conveyed to everyone, including that the right approach to avoid falling prey was to have strong passwords and not to click on untrusted links. What was missing, though, was the direct linkage between the action and the consequence. It is important to state that even with the tactile approach, one experience is not enough. Repetition is important in sustaining positive behavior, for it is only through repeated lessons over time that we will permanently change for the better.
The consequence of poor security choices was not readily apparent as a result of the bad behavior and, therefore, was not sufficient to convince the user to change it. In hindsight this makes perfect sense. If one clicks on a malicious link but does not see any negative consequence of this action in the immediate short term, why would that behavior need to change? Rarely does a message appear on a computer screen announcing the machine has been hacked. In fact, in some of the most successful cyber attacks, the victim never knows that they have been breached and that a cyber criminal has obtained full access to the computer with all rights and privileges. Suppose the computer physically combusted into flames when a user clicked on a bad link—then the user would most likely think twice before clicking in the future.

In the phishing exercise described above, the tactile approach seemed to have the biggest impact, providing a deeper and more meaningful understanding of consequences of actions. That immediate and direct relationship between what one does and its effect is very powerful.

4.2. Recommendations on Fostering Positive Behavioral Changes

The following are basic recommendations to address the human factor of cyber security and incentivize end users to adopt positive behaviors:

• Make it clear that cyber security is a shared responsibility.
• Understand that everyone will not do the right thing all the time.
• Expect and plan for the unexpected.
• Recognize that the human factor plays an important role in the security of the organization.
• Do not rely only on verbal or written communications or directives, especially where critical operations are involved.
• Address the human factor by changing behaviors through a tactile approach.
• Reinforce tactile learning through repetition.
• Be creative in communication and training techniques – making a situation real and demonstrable is essential for learning.
• Connect the dots between actions and the consequences. This provides tremendous motivation for changing behavior positively.

5. Leadership

If there is to be true behavioral change, it has to come top-down from the boardroom level. Leadership is essential in promoting positive change. In order to encourage leaders to become champions of cyber security, it is critical that the issues are presented in a clear and understandable manner. Plain speaking about how to protect, defend, respond, and recover from cyber security incidents can go a long way toward getting leaders to embrace and support the mission. A digital dashboard, for example, is a useful tool that helps visualize complex issues and events, enabling insight to lead to action. Dashboards have become increasingly important for management of complex data across diverse organizational areas, and can help leaders visualize information that will greatly assist their ability to make improved decisions.

The reality, however, is that most public and private sector senior leaders are not cyber security experts, suggesting that something as abstract as cyber security can be overwhelming and hard to grasp. There are no crystal balls as to the when, who, how,
where, and what of an attack. Visualizing these hard-to-grasp issues through a dashboard makes them more real, more readily understood, and promotes positive behavioral change. Additionally, dashboards can quantify over time the progress that an organization has made to a more secure state.

5.1. A Case Study on Using Dashboards to Visualize the Cyber Environment

An exemplary model of a secure dashboard used by an organization contained cyber security information occurring across different organizations and sectors. A major feature included an interactive mapping function that maps actual cyber attacks and depicts the location of attacks from source and destination. Networks and systems linked to critical infrastructures, including utilities, communication, finance, energy, and transportation, are at greatest risk. These systems have shifted from stand-alone air-gapped systems to Internet-connected ones. Consequently, the threat posed by determined bad actors has grown.

By implementing the dashboard, leaders can begin to see potential threats occurring in other jurisdictions that may have otherwise gone unnoticed in their organization. Using a geographic information system interface would enable an organization to overlay both man-made and natural events. The importance of understanding and literally seeing the relationship between the physical and cyber domains cannot be overstated.

5.2. Recommendations on Effective Use of Dashboards

This two-step plan can help leaders better understand and visualize their organization’s networks, complex issues and events, and the information needed to make improved decisions:

- Visualize the information by using a mapping technology that relates physical and cyber issues.
- If there is a cyber event occurring, create a visual representation and show how it is impacting both physical and cyber assets. This will greatly enhance the understanding and importance of the event.

Recommendations and Conclusions

Cyber threats facing organizations in both the public and private sectors will continue to increase in volume and complexity. This ever-changing environment demands constant vigilance and, while there are some sophisticated solutions, there are many simple steps organizations can take to shore up defenses. Measuring progress is essential. The key is to focus on actions, deal with facts, and change negative behaviors. The following summarizes an implementable blueprint of fundamental practices that can truly have a significant impact on an organization’s ability to detect, protect, respond to, and recover from cyber incidents:

- Recognize that there is no 100% guarantee of security, but there are many layers that can—and must—be implemented to strengthen readiness and response.
• Start with understanding an organization’s environment. Make a baseline assessment of the network and of what is running on it. Assets cannot be protected if they are unknown.

• Identify a strategy and cyber security standards with a minimum level of security protection and preparedness acceptable for the organization. Implement this strategy to the predefined level, raising the bar over time toward a more advanced state of protection. Make sure that the strategy includes some of the top Strategies to Mitigate Targeted Cyber Intrusions and the Twenty Critical Security Controls for Effective Cyber Defense.

• Develop a deliverable-oriented action plan. Prioritize tasks—identify, on one side, those areas of greatest need (those so vulnerable that they must be fixed regardless of the cost) and, on the other side, those that are easy and cost little or nothing to remediate, and then work toward the middle.

• Modify the strategy over time as necessary.

• Conduct a gap analysis to measure current status and develop a path forward. Implement an on-going inventory assessment and modify the approach as the threat landscape changes. Flexibility is key.

• Create a safe environment for employees that fosters actionable and timely information sharing and reporting of suspected and confirmed incidents.

• Lead by example; make sure actions clearly demonstrate a collaborative and cooperative approach.

• Recognize that any successful plan must address the human factor.

• Establish concrete, measurable, and attainable metrics to assess progress.

• Develop prospective metrics to influence positive, long-lasting behavior focused on best practices for cyber security.

References


