CREATING A CYBERSECURITY STRATEGY FOR HIGHER EDUCATION

By Don Welch
cybersecurity leaders in higher education spend only a small percentage of their time developing strategy, but this activity is likely to have the largest impact on their institutions. Having a strategy that evolves to adapt to a changing environment can make a good security team into a great one. A well-thought-out strategy empowers the institution to act in alignment with itself, efficiently moving toward common goals.

Most of us don’t know how to create an effective cybersecurity strategy. I certainly didn’t. After many years of trying to fit cybersecurity strategy (square peg) into either an IT strategy or a business strategy approach (round holes), I realized that cybersecurity differs enough from both IT strategy and business strategy that the traditional approach won’t work.

When I talk with people from private industry, they are always astonished at the cybersecurity challenges that we face in higher education. Generally, they don’t realize that we face nation-state actors and that colleges and universities are essentially small cities with almost every kind of critical and sensitive data there is. Mixing in higher education’s core values of autonomy, privacy, and experimentation presents significant challenges in cybersecurity.

The first step in facing these challenges is developing and executing a workable strategy. Many approaches that people call strategies really are not. These include “risk-based security programs” or even “risk-based strategies.” Risk is just one component of a strategy. Focusing only on risk leads to tactical decisions. Other components include increased regulation and compliance standards. Meeting regulatory and compliance requirements should be a strategic goal, but again, this should not be the strategy itself.

**Strategy Definitions**

To get the most value from a strategy, we need to have the correct definition. *Strategy* started as a military term in the eighteenth century but has been in use as a concept since organized warfare began. Generally, strategy involves allocating a nation-state’s resources toward winning a war as opposed to winning a battle. In the late twentieth century, business began to adopt the term. Even though the environments are vastly different (of course), the concept does translate well to the business environment.

Below are three common definitions of *strategy* from a business perspective. Though all three are valid, they all are also incomplete. Therefore, I’ll combine them into a single definition that best fits cybersecurity. First, the most-recent *Wikipedia* definition of *strategy* is: “A high-level plan to achieve one or more goals under conditions of uncertainty.” This is a good start. Cybersecurity is the poster child for conditions of uncertainty. However, we need more from a strategy. Second, Henry Mintzberg calls *strategy* “a pattern in a stream of decisions.” This definition captures the concept that a strategy should drive alignment throughout an organization—a concept that is foundational to success, in my experience. Third, *Business Dictionary* defines *strategy* as “planning and marshalling resources for their most efficient and effective use.” This idea of allocation or prioritization of resources is a critical component. Thus, I combine all...
three of these and define \textit{strategy} as follows: “A long-term plan that allocates resources and sets a framework for decision-making to achieve long-term goals under conditions of uncertainty.”

\textbf{Business Strategy}

Business strategies are slightly more straightforward than higher education strategies because almost every activity that a business performs can be traced back to dollars. An activity is either a cost or a revenue, and businesses aim to maximize profits. Colleges and universities are different. They must have more revenue than expenses, but in higher education, surplus dollars do not necessarily mean that an institution is performing better. The definition of success is stakeholder value, making the success of a college or university much more difficult to track.

Michael Treacy and Fred Wiersema talk about three types of business strategy: customer intimacy; product leadership; and operational excellence.\textsuperscript{4} Each offers a framework that is consistent with the definition of \textit{strategy} stated above. Businesses executing a \textit{customer intimacy} strategy focus their resources on the customer experience. Nordstrom was famous for this approach; a resurgence of this line of thought is evident in retail today. To compete with online shopping, many retail companies are focusing on a customer experience that online sellers can’t provide. Second, businesses that execute a \textit{product leadership} strategy are providing a product or service that is better for some segment of the market than that of any competitor. Apple under Steve Jobs is an example. Apple invested a great deal into R&D, and accounts of Jobs’s attention to detail and the focus of the Apple design teams illustrate the company’s slavish devotion to this strategy. As a result, those who believe the iPhone is the best smartphone will pay a premium. Finally, companies that focus on an \textit{operational excellence} strategy deliver products or services at prices lower than those of their competitors. Walmart is a classic example.
If you squint your eyes, you might be able to see how a cybersecurity strategy could be devised to fit one of these patterns. But doing so would not be intuitive.

**IT Strategy**
The Wikipedia definition of technology (IT) strategy is: “the overall plan which consists of objectives, principles and tactics relating to the use of technologies within a particular organization.” TechTarget states that IT strategy is a “comprehensive plan that outlines how technology should be used to meet IT and business goals.” The main concept to note is that IT strategy is not adversarial or competitive per se. In business strategy, by contrast, companies are striving to succeed over competitors. IT strategy must support the company strategies and deliver what the company needs.

Many IT strategies are simply tactical checklists of best practices. This represents an operational efficiency approach. IT strategies generally involve the prioritization of resources both within the organization and within the IT department. The long-term goals usually fall into two categories: those that enable a business goal, and those that free resources for business efforts. For example, a retail business may have a customer intimacy strategy. To execute this strategy, it may choose to collect and analyze data. The company may decide to increase the investment in information technology in order to increase the delivery and quality of information as a business goal. An example of a strategy to free resources would be IT consolidation that might trade a decrease in responsiveness for resources that can be spent elsewhere.

Risk must be part of the IT strategy. Risks include obvious ones such as disaster recovery and business continuity. Risk management involves determining how much risk the business can tolerate versus the costs required to address those risks. Availability is also a central tenant of cybersecurity. Confidentiality, integrity, and availability risks are the core of cybersecurity, so this is the obvious place where the IT strategy and the cybersecurity strategy overlap and must be aligned. However, making the cybersecurity strategy part of the IT strategy is a mistake. The two functions are too different to be fully integrated.

**Strategic Analysis**
Strategic analysis in business is usually organized into strengths, weaknesses, opportunity, and threats—aka SWOT analysis. SWOT analysis will work for cybersecurity, but it feels forced to me. There are three characteristics of cybersecurity that suggest a different approach. First, cybersecurity will always be a function of the organization’s strategy. Second, cybersecurity is reactive and not proactive. Finally, cybersecurity is asymmetrical.

_Cybersecurity will always be a function of the organization’s strategy._ The purpose of cybersecurity is to protect the information assets of the organization. An organization owns information assets so that it can accomplish its mission and give it an advantage over its competitors. According to Bill Stewart and his co-authors, two questions are the key to developing a strategy: (1) “How does cybersecurity enable the business?” and (2) “How does cyber risk affect the business?” Like IT strategy, a standalone...
cybersecurity strategy would not make sense. The accusation “security for security’s sake” would ring true. A cybersecurity strategy must complement the overall strategy as well as the IT strategy.

Cybersecurity is reactive and not proactive. Many experts have encouraged us to think proactively about cybersecurity and have called their strategic approaches proactive. Maybe it’s semantics, but for me there is a difference between acting proactively in a tactical sense and having a proactive strategy. We can’t seek out bad guys and arrest them or destroy their capability before they attack us. To me, a proactive strategy means acting before our adversaries do—either to beat them to a goal or to degrade their ability to obtain their goals. We can prepare for attacks before they happen, but we can’t act until they occur. Our adversaries still pick the time, the place, and the method of attack.

Cybersecurity is asymmetrical. This is because our adversaries have options that we do not. We must operate within a legal framework that limits what we can do. Our goal is to defend our information. Our adversaries’ goals are to steal or change our information or to stop us from having access to it. An analogy is a guerrilla war where the conventional forces are trying to defend territory and population while the guerrilla force is trying to gain political advantage by attacking the conventional force and civilian infrastructure.

Rather than considering SWOT, cybersecurity strategic analysis should look at threats and constraints. Essentially, the purpose of a cybersecurity program is to mitigate the threats it faces while operating within its constraints.

**Threats**

Whereas others might use the term risks, I’ll use the term threats. This implies that there is a thinking and reactive adversary on the other side. We are looking at adversaries and what they might try to do to our college or university. We must know what it is that adversaries want to attack. What is valuable to them? How valuable is that information to them, and how much effort is required? The answers to those questions determine the likelihood that an attacker will go after that information. We must also look at the impact of a successful attack on our institution.

If our adversaries succeed, what will be the impact?

\[ \text{Threat} = \text{Impact} \times (\text{Value} / \text{Effort}) \]

This formula is actually a qualitative analysis. Of course, we all would love to have data that could be used to quantify risk. However, when we rely too much on metrics to calculate risk in cybersecurity, we get precision but not accuracy. We get numbers that we can measure, calculate, and compare, but these numbers might lead us to the wrong conclusions. Take the number of compromises, for example. If the number of compromises per month is dropping by 5 percent, does this mean that our security is getting better? Or does it instead mean that our adversaries have adapted, and we aren’t detecting compromises? Or does it mean that our adversaries have moved to different activities but will be back in the future? Also, the data that we gather is usually based on assumptions. Too many events in cybersecurity are “black swans”—unpredicted by previous events. Metrics can be useful and helpful, but they must be incorporated into reasoned qualitative judgment.

Table 1 shows another way to view this formula/analysis.

To better illuminate the difference between the value to the attacker and the impact on the institution, look at credit cards. Attackers can make good money from stolen credit cards whether they sell the cards or use the cards themselves. Stealing credit cards is worth a lot of effort. But individuals are liable for only up to $50 if their credit card number is stolen. Likewise, a college or university storing credit card data that is stolen has no impact from the theft. The credit card providers are the ones who lose. The Payment Card Industry Data Security Standard (PCI-DSS) uses fines, the threat of increased process, or the revoking of card-processing privileges to create an impact on the institution, pushing colleges and

<table>
<thead>
<tr>
<th>Table 1. Threat Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Category</strong></td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>Low</td>
</tr>
</tbody>
</table>
universities to expend the effort necessary to protect the cards.

A good cybersecurity strategy focuses on identifying the largest (high-impact) threats in order to garner the resources to protect the institution and defend against those threats.

**Constraints**

We all know what we’d do in a perfect world, with unlimited funding, complete cooperation, and as many talented staff as we need. Since we don’t live in a perfect world, the cybersecurity strategy must focus on those threats that have been identified as the most serious (as noted above) while considering the numerous constraints limiting cybersecurity programs in higher education.

- **Funding.** This constraint is fairly straightforward. It concerns capital, operating expenses, and the amount and timing of money that can be spent.
- **Regulations and Laws.** The cybersecurity program must be compliant with regulations and laws. Resources expended for compliance are not available for other purposes.
- **Staff Time and Talent.** The capacity/capability of current staff and the ability to hire and retain talent are both limited. High turnover due to IT markets, the pay that can be offered, and the capacity of staff to learn new skills are all examples of restrictions around staff time and talent.
- **Business Overhead.** The individual culture of various groups in a college or university will determine how much can be accomplished through security controls. For example, understanding that the finance team will tolerate a lot of overhead whereas clinical physicians will tolerate very little is important. The process of assigning high-, medium-, or low-tolerance ratings for the various groups can provide better insight into an organization’s overall tolerance for security overhead.
- **Political Capital.** This constraint overlaps a bit with business overhead, but the emphasis here is on leadership and peer support. For example, if a college or university recently suffered a major security breach, the security team may have a good deal of political capital with senior leadership. In addition, knowing how much those in the rest of the institution trust the security team—that is, the level of peer support—is critical. I recommend making a list of the key leaders across the institution and categorizing them as “will support with a solid case,” “can win support,” or “tough sell.”
- **Accountability.** This could be a subcategory of political capital, but I feel it deserves its own discussion in higher education. Being aware of the culture of accountability in an institution is critical to developing a successful cybersecurity strategy. If a strategy depends on shadow IT, but shadow IT is never disciplined for ignoring a central edict, the strategy is in trouble. Are there any real consequences to ignoring cybersecurity? The answer to that question will affect the cybersecurity strategy.
- **Calendar Time.** This constraint includes the dates that capabilities must be in place and the resources that are available.

---

**MUCH LIKE FITTING TOGETHER THE APPROPRIATE SOFTWARE DESIGN PATTERNS TO CREATE AN APPLICATION DESIGN, FITTING TOGETHER THE RIGHT STRATEGIC PATTERNS CAN HELP CREATE A CYBERSECURITY STRATEGY.**
Not everything in the cybersecurity strategy will be time-critical. This constraint is best analyzed in two parts: (1) identifying any and all limitations on time; (2) sequencing decisions to include calendar time considerations.

- Governance. If governance is imposed on cybersecurity, then it is a constraint. If governance can be created by the chief information security officer, then it is a component of the cybersecurity strategy. With a trusted security team, governance could be as lightweight as a reporting line. Most security teams in higher education don’t have that luxury, however. In this case, advisory committees, with their transparency and participation, are great ways to build trust and support. Heavier governance can involve an oversight committee, with many subcommittees and an executive committee. In a lower-trust environment, the oversight committee will make decisions and approve major projects. Heavy governance will be slower, more time-consuming, and more restrictive. On the other hand, the security team will have more support and will be able to impose more overhead, and the rest of the institution will be more accountable.

**Strategic Patterns and the Cybersecurity Strategic Matrix**

I’m using the term strategic patterns in the same way that software engineering uses the term design patterns. Software design patterns themselves can’t be used to create an application; instead they serve as a component of the application design. Likewise, strategic patterns function as one part of the overall cybersecurity strategy.

Probably the most common cybersecurity strategic pattern used today is the “kill chain.” Another is “Defense in Depth,” which first came into favor in the 1990s. People-centric patterns were more popular a decade ago but are still important. Process-centric patterns are common and may be appropriate depending on the maturity of a cybersecurity program. Technology alone is unlikely to solve all our problems, but understanding what we need technology to do and its relationship with resources is a critical part of any cybersecurity strategy.

Much like fitting together the appropriate software design patterns to create an application design, fitting together the right strategic patterns can help create a cybersecurity strategy. A collection of cybersecurity strategic patterns forms the high-level strategy. Moving down a layer will involve people, process, and technology. A matrix is the natural way to capture this level of the strategic plan. Should people be emphasized over process? Which technology will be chosen? A cybersecurity strategic matrix can capture as well as analyze these decisions.

Table 2 shows a matrix with the five high-level cybersecurity strategic functions from the National Institute of Standards and Technology (NIST) Cybersecurity Framework—identify, protect, detect, respond, and recover—on the left side and with people, process, and technology across the top. This visual representation shows how the five functions are being addressed and the trade-offs that are being made. The five top-level functions could also be subdivided into more areas. For example, protect could be detailed as access control, awareness and training, data security, information protection processes, maintenance, and protective technology.

Based on the cybersecurity strategic patterns chosen, projects or initiatives can be inserted into the cells. These projects or initiatives represent the resources that are required. Doing this will necessarily prioritize the functions and how they will be addressed. For example, if the Kill Chain pattern is used, then the detect function(s) will probably be a top priority. A Defense-in-Depth pattern will require more effort in the protect function(s).

Next, efforts should be prioritized among People, Process, and Technology. For example, a startup that has a small, dedicated staff, that doesn’t have much money, and that must be highly productive will look first at solving issues with people. By contrast, organizations that are very mature can look to process first for success. Here is another example. The Identify function includes asset management, which requires inventorying hardware, software, external systems, and data flows. These needs can be addressed by people, process, or technology but most likely by a combination of all three. People can provide inventory information. Process can issue an “authority to operate” and require documentation. Technology tools can perform automatic discovery of hardware and software. There are trade-offs in each of these approaches.

Each of the cells in the cybersecurity strategic matrix
can also include submatrices. For example, the Detect/Technology cell could hold a matrix detailing Network, Payload, and Endpoint detection functions across Real-Time/Near-Real-Time and Post-Compromise technologies. Or the Protect/People cell could include a matrix dividing People into Users, IT Staff, and Security, with Mandatory and Optional functions. The idea is to make clear the tradeoffs involved in the allocation of resources.

Another way the cybersecurity strategic matrix can be helpful is in understanding emergent priorities and patterns. As tradeoffs are made in order to allocate resources within constraints, it may become obvious that the initial thoughts and plans simply aren’t practical. A better way to abstract resource allocation, or a different strategic pattern, may become clear. These insights will be important in communicating the cybersecurity strategy.

Communicating the Cybersecurity Strategy
The implementation of a successful cybersecurity strategy depends on a wide variety of stakeholders. For the strategy to be useful to others across the college or university, they must act in alignment with it. Yet communicating the cybersecurity strategy throughout an institution can be challenging. People in different roles need different levels of understanding. End-users will be the least sophisticated security-wise, whereas the security team must of course understand the details. In between are the system administrators, developers, academic leaders, and more. The cybersecurity strategy must be communicated in multiple ways tailored for everyone in the institutional audience.

Creating a cybersecurity strategy that serves as a framework for decision-making requires a concept simple enough that people can hold it in their head. What does this mean in practice? The strategy description must fit easily on one PowerPoint slide. There are two effective ways to do this. Both methods can be incorporated into a two- to five-minute presentation that will create a memory aide for the audience.

One way is to use the old standby of bullet lists, phrasing the text so that it captures the essence of the strategy. The range should be three to seven bullets, with five being optimal. A word or two followed by a phrase or sentence gives the viewer something to hold on to. For example: “Information Centric: Categorize and prioritize defending high-risk information.” It should be possible to explain the strategy in five minutes—not quite an elevator pitch, but not much more.

The other, perhaps better method is to use a diagram. The combination of a graphic and words is easier
for someone to remember than just text. This might be hard if you’re not an artistic person, but communication teams may be able to help. The risk is greater if the diagram doesn’t hit the mark, but the possibility of a winning home run is greater as well. Figure 1 is the illustration I use to communicate Penn State’s cybersecurity strategy.

These basic explanations might be the most important part of a cybersecurity strategy. Unfortunately, they are, like a poem, the hardest to get right. As the saying goes, a poor plan well-executed beats a great plan poorly executed. This simple, high-level explanation of the cybersecurity strategy will play a large part in determining how others across the institution do (or don’t) align.

Still, for those who want additional details and who have the tolerance to read or listen to more, further explanations are required. A “one-pager” is an option. This is a document that explains the strategy on one side (or both sides) of a piece of paper. Another option is a fifteen- to thirty-minute strategy briefing. This could consist of seven to fifteen slides that put more flesh on the bones of the strategy. The higher the picture-to-bullet ratio, the more effective this communication will be. I also suggest including a discussion of the threats and constraints. The more comfortable people are with the reasoning behind the strategy, the more enthusiastic they will be in implementing it.

Depending on the institution, a well-polished explanation of the cybersecurity strategy may not be required. The main benefit comes from the writing. Chances are that the detailed justifications will be helpful, at some point, for various initiatives.

I believe that effective communication is perhaps the most critical aspect in the entire process of creating a cybersecurity strategy. Feedback is thus essential. Words and concepts that make perfect sense to the security team, for instance, may be lost on some stakeholders or, worse, may evoke a bad reaction. Communication will need to be modified over time.

**Conclusion**

Thinking about cybersecurity from solely a risk-based perspective or as the risk part of an IT strategy will not result in the most efficient allocation of resources, nor will doing so align the institutional cybersecurity efforts. Cybersecurity demands a strategic approach because it is difficult, rapidly changing, and potentially devastating to a college or university. Cybersecurity differs from either IT or business operations because it is adversarial, reactive, and asymmetrical. Cybersecurity efforts must be closely aligned to the institution’s overall strategy and must complement its IT strategy. Failure to think and act strategically results in the inefficient use of resources and increases institutional risk.

The inputs to cybersecurity strategy are threats and constraints. The strategy must identify the institution’s information assets and the impact of a successful attack on them. Understanding the value to attackers provides insight into the likelihood of attacks and how much effort adversaries will expend to gain those assets. This analysis provides a risk-based prioritization for defending information. Institutions have limited resources to expend on cybersecurity. These resources include not only funding and staff but also intangibles like political capital and accountability. An effective strategy must address the most serious threats while staying within the constraints of the institution.

Cybersecurity strategy must be long-term, be effective under uncertainty, prioritize resources, and provide a framework for alignment throughout the institution. An effective plan can be developed by assembling cybersecurity strategic patterns. In addition, a matrix that matches the functions of the NIST Cybersecurity Framework to people, process, and technology can provide a visual representation of the strategy.
representation of the implementation of the cybersecurity strategy. Finally, sequencing the contents of this matrix can create a roadmap of projects, initiatives, and efforts to execute the strategy. Beyond offering a risk-based approach, the strategy will effectively allocate resources and align efforts.

Cybersecurity is not just an IT function; it is an institutional function. Thus, almost all members of the college/university community have a part to play and should act in alignment with the cybersecurity strategy. And since they can’t align with the strategy unless they understand and remember it, communicating the strategy is as important as devising the strategy itself.

Cyberattacks on colleges and universities are increasingly frequent and damaging. The cyberthreat to higher education overall is both significant and likely to grow for the foreseeable future. Meeting the challenge, especially in higher education, requires strategic thinking, and that strategy must come from cybersecurity-specific strategic thinking.

Notes
9. For examples, see: John M. Gilligan, slide 3 in “Top Level Cybersecurity Strategy,” presented to AFFIRM, February 17, 2010; Office of the State Information Officer, Oregon, Figure 3, “Public Cybersecurity: Classes of Interventions” (p. 11), in “Implementation of E.O. 16-13: Unifying Cyber Security in Oregon” (2016); National Institute of Standards and Technology, Figure 2, “Notional Information and Decision Flows within an Organization” (p. 13), in “Framework for Improving Critical Infrastructure Cybersecurity,” Draft Version 11, January 10, 2017.

© 2019 Don Welch. The text of this article is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License.