From Bolted-On to Baked-In: Designing Cybersecurity into Digital Offerings[1]

Dr. Keman Huang and Dr. Keri Pearlson
Cybersecurity at MIT Sloan
January 28, 2021

Understanding how suppliers build cybersecurity into their digital offerings has never been more topical. As evidenced by the SolarWinds supply chain cyber-attack, our products are only as secure as the weakest link in our supply chain. Likewise, our customers are expecting our digital offerings to be secure as they incorporate them into their offerings. But as recent history has shown, designing and building secure digital products and services is not without significant effort.

Adversaries are able to identify the vulnerabilities embedded within digital offerings with the support of a robust cyber-attack service ecosystem.[2] Company leaders must respond along multiple avenues to ensure their offerings are not vulnerable. Many mechanisms such as cybersecurity training and education, implementing the security development lifecycle process, developing automated vulnerability discovery tools, and setting up bug bounty programs[3] have been used, however, vulnerabilities within digital offerings still persist. The number of discovered vulnerabilities within the National Vulnerability Database is increasing yearly, 18,356 new vulnerabilities were reported in 2020 alone,[4] and it is likely that there were significantly more which remain unreported.

Our research studied how companies build products and services, often called offerings, that were cyber secure. We wanted to know if product developers built in cybersecurity from initial design or if security was somehow added later. We leveraged our cybersecurity culture model[5] to frame a qualitative study of three large, well-known global companies: one provides telecommunication services and products; one provides energy and digital automation solutions; and one is an energy provider in which digital solutions are developed to support their business. By conducting one-on-one, 30-to-45-minute, in-depth, semi-structured interviews with 44 employees occupying different positions across these companies, we studied how product development teams build cybersecurity into their offerings and what mechanisms have been developed to promote such behaviors. Further, we hosted several workshops to discuss and validate our findings with senior executives and managers from both product development and

[1] The authors wish to thank Abigail Kolyer, MIT research assistant, and George Wrenn II, advisor, for their assistance with this research. Thank you also to the numerous product development professionals who generously gave of their time to be interviewed as part of this project. Funding for this project was from Cybersecurity at MIT Sloan (CAMS). All authors contributed equally to this project.
[2] Huang, Keman, Michael Siegel, Keri Pearlson, and Stuart Madnick. "Casting the dark web in a new light." MIT Sloan Management Review 60, no. 4 (2019): 1-9.
[3] Ryan Ellis, Keman Huang, Michael Siegel, Katie Moussouris, and James Houghton, " Fixing a Hole: The Labor Market for Bugs," in New Solutions for Cybersecurity , MIT Press, 2018, pp.129-159
[4] https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all;
[5] Huang, Keman, and Keri Pearlson. "For what technology can't fix: Building a model of organizational cybersecurity culture." In Proceedings of the 52nd Hawaii International Conference on System Sciences. 2019.

cybersecurity areas in the three global companies, as well as other Fortune 500 companies, and cybersecurity solution providers.

We found that building cybersecurity into offerings did not happen naturally in the design phase of the offerings. That was surprising since executives and business leaders increasingly realized the importance of cybersecurity for their companies and thought their teams did too. When talking about digital offering development, leaders tended to mention cybersecurity as a high priority, but it got lost during execution. Behaviors such as expecting development teams to organically design offerings without cybersecurity vulnerabilities or expecting these teams to invest time and resources in cybersecurity education without appropriate support is unrealistic and unlikely to be fruitful. Instead, organizations need a holistic organizational mechanism that involves not only the developers, but all key stakeholders including managers, executives, communities, customers and suppliers. Our main suggestion is that cybersecurity must not be bolted-on to an offering after initial development, but baked-in the digital offerings from the very beginning of the design. To reach that goal, executives must build a culture of cybersecurity within their product development teams that drives cybersecurity considerations in their design behaviors.

Cybersecurity is not the top priority for digital offerings

When asked, few will deny the importance of cybersecurity for digital offerings however, in practice, product teams tend to downgrade the priority of cybersecurity. Our study revealed three ***mindsets*** that combine to reduce prioritizing cybersecurity in digital offerings in the initial list of features and capabilities.

Mindset #1: Cybersecurity does not directly contribute to revenue

Nothing is more important to a business's livelihood than revenue generated from offerings. Hence, when resources are constrained, product teams readily cast aside any features that cannot directly contribute to revenue. Unfortunately, cybersecurity has not been considered a direct revenue contributor. Our study revealed a widespread belief that customers expect cybersecurity within digital products, but ultimately pay for product features and solutions that add value, reduce costs, or provide competitive advantages, as those are clearer indicators of value. In other words, many executives believe that customers will not pay for cybersecurity within digital offerings, but they expect it to be there. In our interviews, we heard comments such as,

> "*Most customers expect security but don't understand it. Customers treat cybersecurity like tires on a car. They expect it to be there, but they are buying the product because of the features and solutions they want.*"

Interviewees also told us that functional features will always outweigh cybersecurity. "*If the product isn't built with certain features, it doesn't matter how secure it is*". When product teams need to make tradeoffs among many considerations due to the market pressure, they will push back cybersecurity.

The same priorities remain when product teams become customers themselves. When choosing their vendors, including open-source and third-party components, the product teams also prioritized functionality instead of cybersecurity.

> "*You want the latest and greatest offerings with all the best bells and whistles. But it may not have the most timely support for cybersecurity. The features and functionality can outweigh the cybersecurity support because designer don't to lag behind*"

While this may not always be the case, especially as new breaches are found and widely reported. No one wants their company's reputation harmed because of a security breach in a product they sell to customers. But right now, other features take precedence in offering design.

Mindset #2: Cybersecurity can hinder the time-to-market

Building cybersecurity into digital offerings will consume resources, including time and financial investment. Some managers believe that including cybersecurity features into offerings will delay or take resources away from other features and increase the time-to-market. Like feature sets, getting an offering to market takes priority over making the offering secure since a product that is late to market may also lose the market entirely.

> "*If products with all the bells and whistles but misses time-to-market, we miss the opportunity*."

If an offering cannot make it to market quickly enough to meet customer needs or beat competitors, its cybersecurity features do not matter. This mindset means that the team will make sure they only implement the minimal cybersecurity requirements necessary to get the offering out of the door. One interviewee told us, "*What is the minimal cybersecurity I have to do to get the product out the door?*" is the question the team will always ask. Development teams also only include the maximum cybersecurity features that won't slow down their time-to-market. Otherwise, the product team will push back or try to find a way to work around those cybersecurity requirements.

Mindset #3: Lack of cybersecurity within offerings have limited impact until there is a breach

When managers are aware of potential cybersecurity risks in their digital offerings, they underestimate the consequences. One manager told us,

> "*I have no sensitive data within our offering. Even if you breached it, you could not do anything. So, for us, cybersecurity is less critical.*"

The negative impact is also considered as independent and will not influence others.

> "*Our product does not directly connect to our internal system; it is a separate one. If one customer's connection has some problem, the impact would be only to that customer, not to the massive others*".

Cybersecurity can be a moving target, as vulnerabilities evolve. Our study uncovered ideas in development teams that in the early stage, cybersecurity risks would be limited due to low exposure of the offering to anyone outside the project. Further, the developers themselves did not need to design for cybersecurity. There were others on the team who would catch any vulnerabilities later. Cybersecurity risk only needed to be fully considered once the product became a business line that reached customers.

> "*For this particular product, we are looking to test for a market, and only had 6 customers who knew about it. It was a relatively low exposure. As we go through the lifecycle to launch it, security becomes a much more robust conversation. When it is turned into a business we are going to offer, then we need to go through our full process for cybersecurity*".

Given these three mindsets, cybersecurity is not a revenue generator, building with cybersecurity can slow down the time-to-market, and consequences may be limited during the early development stage, it is not surprising that product teams don't make cybersecurity top design priority. Cybersecurity is treated as a

"bolted on" feature for offerings. It is postponed until it may be too late to incorporate into the offering design or forgotten until the last minute when testing uncovers a problem. When designers do not have the right values, attitudes and beliefs and leaders do not follow through to make cybersecurity design a priority, products with security issues will be released to the market, as evidenced by the 6,060 new but vulnerabilities (including the SolarWinds Orion issue) listed in National Vulnerability Database during 2020.

Cybersecurity Must Be Part of the Design Criteria

The atmosphere of cybersecurity for digital offerings is changing. Yesterday's mindsets are no longer sufficient. Increasingly, cybersecurity is becoming a *de facto* requirement. It is expected. As that happens, it also becomes a key selling point. After all, no one wants to buy or use an insecure offering. A cybersecurity vulnerability can result in cascading costs to the whole ecosystem, a hit to the corporate brand, and potentially a legal issue for the manufacturer who designed the offering. Perhaps most important is that the cybersecurity-as-afterthought approach is more expensive than designing security in at the initial design phase and can delay the time-to-market.

Offerings are expected to be cybersecure

Customer increasingly view cybersecurity as a requirement, not just a bonus. Some will explicitly ask for it in or insist that vendors fill out complicated security questionnaires to insure it's there. As more security breaches come to light, customers are less willing to ignore the risk from supply chain threats. The cyber-attack or breach no longer feels like a remote possibility for customers. One manager said that:

> *"Cybersecurity is becoming a huge focus for us because our customers think security is so important. If our product is not secure, it shuts down customer conversation. Security features are a huge selling point for our products."*

Some customers include independent penetration-tests as part of the acceptance process. They use tools to find vulnerabilities, and then request vendors to fix the issues. Even in cases where the customers purchasing the offerings don't request cybersecurity features, often there is a central function within the customer's organization requiring cybersecurity standards be met.

No one wants to purchase a product or service with cybersecurity vulnerabilities that are not addressed. While product owners often want to rush a product to market, insufficient cybersecurity in the product offering will be a deterrent to customers buying them. This is especially true for highly competitive markets where customers have many alternatives. Cybersecurity is already a de facto requirement for critical infrastructure customers such as military and financial services, since these industries are increasingly big targets for cyber-attacks.

Our study also found that offerings with unique market-desirable features require their vendors to have a high level of cybersecurity. "*We definitely want our vendor as cybersecure as we are*" was a common theme we heard when selecting digital offering providers. To achieve this level of confidence in vendor security, cybersecurity was increasingly built into contracts to understand the vendor security practices and to make vendors accountable for cybersecurity risks. These contractual provisions were not negotiable.

"*In our agreement, whenever there is a digital component, there is another layer in the agreement about cybersecurity. Those clauses are considered on a case by case basis, but they are non-negotiable*".

Cybersecure offerings are increasingly required to do business. We have seen cybersecurity become a main selling point for digital offerings, contributing directly to revenue. If a digital offering only has cybersecurity features but no functionality, no one will buy it; but if cybersecure features are lacking, the offering may lose out to competitors.

Lack of cybersecurity within digital offerings has cascaded costs

The lack of cybersecurity within a digital offering affects not only the offering itself, but other offerings from the same company and potentially through the supply chain. Sometimes the corporate reputation is not reparable. For example, the Equifax breach back in early September of 2017 make the company lost its market position and has struggled to recover ever since[6].

Importantly, it does not matter how cybersecurity risks are introduced into customers' systems: whether through a component developed by the product team, or from the adopted open-source components, or provided by third-party vendors. Once there is a brand name on a digital offering, customers will expect the providers to cover cybersecurity and connect it with the provider's brand. Therefore, once a cybersecurity incident occurs with a specific offering,

"*Once there is a cybersecurity incident occurs with a specific offering, it is not only a black eye for that offering. It is a black eye for the whole company, and it ends up toward to other many products to prove that they are secure vs. just one product that is not.*"

Engaging cybersecurity earlier makes the whole product development process more effective

Nowadays, relying on last-minute cybersecurity reviews or pen-tests to identify cybersecurity issues and then fix them, can result in additional work for the development team and delay product delivery. Given the constant pressure to bring the offering into the next step in the development process, development teams often attempt to implement temporary solutions or workarounds so that they can move on in the process, whether it fixes cybersecurity issues or not. Without addressing the root vulnerabilities, cybersecurity issues will come back down the road.

Additionally, there are not always viable solutions for the identified cybersecurity issues, short of rolling back to rework the core functionality, or even architecture. One security manager elaborated.

"*Without cybersecurity as part of the design early on, it is very likely that we would have those basic fundamental cybersecurity problems in the early version of the product. They will not be detected early in the development process. But once those deficiencies are realized, we are certainly not able to release the product out to the public without a substantial redesign.*"

Finally, the cybersecurity-as-an-afterthought approach can even cause friction between developers, designers, and cybersecurity architects. We heard such complaints during our study:

[6] Keman Huang, Stuart Madnick, "A Cyberattack Doesn't Have to Sink Your Stock Price", Harvard Business Review, 2020.

> *"The cybersecurity architects include so many cybersecurity controls that the system is no longer high performance. They destroy the product, and the users are not happy.*"

In extreme cases, if cybersecurity is not included when designing the product, the effort to bolt on cybersecurity can make the designed digital offering no longer economically feasible.

> "*Cybersecurity did modify the business case and the economy. We need to have this feedback to refine the business process. At some point, it may make the ROI [Return on Investment] too low for the corporation to move ahead*".

Challenges for building cybersecurity into offering development

Our research suggests that baking-in cybersecurity from the initial design stage, rather than bolting-on later, is the best approach for creating cybersecure offerings. To do that, leaders must change the three mindsets described above. But this is not easy or straight forward. Our research uncovered several challenges to be managed.

Challenge 1: Cybersecurity is dynamic making offering design complex

When managers want to include cybersecurity measures they are hindered by complexity. Instead of working through the extensive requirements, designers prioritize aspects of products that are more easily defined. As one manager described this as

> *"People don't intend to 'not care' about security. But a lot of the production environments are so complicated that the high priority is to make sure the product is not vulnerable to something specific, and maybe by focusing on that you miss something from a security standpoint."*

Such specificity of certain fixes can distract from a broader initiative to implement cybersecurity throughout the entire lifecycle, though this is still a better alternative than ignoring security entirely.

Understanding and dealing with this complexity requires significant experience and knowledge for product developers. One designer explained,

> "For *People who want to focus on cybersecurity implementation, it takes them 3 years to get very good and very familiar with what needs to be done.*"

With the many aspects of cybersecurity and the dynamic nature of new threats, expertise is not easy to obtain.

> "*There are over 200 security requirements. Normally between 70-120 apply to any product. There is not one person who is an expert on all 200.*".

Even when a team has the cybersecurity capability for the initial design, as product specs change, new cybersecurity expertise may be needed. For example,

"*For a team who were competent to do the cybersecurity for the existing product, when they added a web interface, they had to take on 30+ cybersecurity requirements. It was a new area for them. They didn't have the skills there.*"

The turnover of developer teams further adds challenge, requiring a more sustainable way to train the product team and carry on the institutional cybersecurity knowledge.:

"*You can train someone to do cybersecurity but then they may move. The turnover makes it difficult to have sufficient security built in. Contractors are particularly difficult. The turnover is hard to overcome.*"

Importantly, cybersecurity requires a unique way of thinking. *"Cybersecurity is a foreign way to think for many developers*", explained one cybersecurity professional we interviewed. Generally speaking, developers tend to think about building their offerings, while cybersecurity is more about how the product might be destroyed or manipulated. Cyber attackers work by their own rules and attack in ways that you may don't even think about. A manager shared one example:

"*An ATM vendor asked a safecracker to break into their ATM, and they were expecting someone to use the keypad, but the cracker pulled out a hammer and smashed it*".

Hence, the complexity to bake-in-cybersecurity requires a team, not just product developers or designers, to bring in sufficient and sustainable cybersecurity expertise and thinking to make sure offerings are cyber secure. This will require business leaders and executives to enhance cross-functional collaborations systematically and consistently.

Challenge 2: Designing security into offerings is often managed by a parallel security development process, which can be expensive and inefficient

As executives realize the importance of building cybersecurity into digital offerings, our research shows they often rely on a cybersecurity development lifecycle (SDL) process. While SDL can ensure the offering is designed as securely as possible before it gets to the marketplace, it involves significant investment in coordination between the offering designer and the SDL team. Further, it can give the designer the impression that someone else is responsible for security and result in security being bolted on later in the process rather than baked in from the beginning.

SDL is a tool for product teams that engages the necessary cybersecurity resources to ensure the right level of cybersecurity is built into products. However, in practice, SDL can be burdensome and in some cases, it's only seen as a way to due diligence. SDL does force the designers to document security considerations, but the burden comes in when the process requires an enormous amount of "paperwork". While it does force the designers to document security considerations, we consistently heard complaints when we discussed the adoption of SDL with the product teams.

"*Our SDL process want each team to provide artifacts. Managers want a paper trail. I worry that it will slow the process down to where you are non-competitive but not really improve cybersecurity."*

The dynamic nature of cybersecurity means that the SDL must also adapt regularly. Changing requirements create friction between the security team and the developer team while also increasing distrust of the SDL.

> "*If you talk with the cybersecurity team, you will get a story one day but another story the other day as things keep changing. I don't know how they all fit together. Maybe they can streamline it or be more holistic and efficient.*".

This results in internal tension and discussion about who should take responsibility for the cybersecurity requirements of offerings.

> "*There is an internal debate between the engineering team and the security team on who has the responsibility to make the compliance with the SDL happen. They are pushing it off. We are dealing with this weekly."*

Without someone taking personal responsibility for the security aspects of the development process, SDL become a set of standards and compliance requirements that just must be checked off.

> "*Developers do whatever they are told to do to check the box without understanding what the cybersecurity requirement really is, so that they cannot fully build cybersecurity into the product.*"

Further, when security is just a set of standards and requirements on a list to be checked off, the product team devalues the importance of the SDL process. These behaviors can be dangerous as the product team will just focus on making sure they are doing the SDL process correctly, instead of understanding what they are doing and why. One interviewee told us about such a situation:

> *"We work with internal security advisors to make sure we are doing the SDL process correctly. To make sure we do the right things and implement the cybersecurity requirement correctly, we look for an external resource rather than spend our own time on it. We just need to get it done so we can focus on other aspects of the development process."*

To drive designers to bake in security from initial design processes rather than just go through the motions of the SDL process, executives need to design a holistic solution which can make it as easy as possible for the developer team to implement cybersecurity appropriately. Instead of bolting on an SDL process, developers must have the attitude that it's their responsibility to design both elegant and secure offerings and use the SDL process to enhance and reinforce security solutions.

Challenge 3: The leader's stated priority for cybersecurity does not match their behaviors

A third obstacle is the inconsistency between words and actions within the organization, especially from top management team. While most executives claim to prioritize cybersecurity from both a technology and cultural standpoint, the reality can be more complicated. Despite a company-wide sentiment to build products that include cybersecurity, in reality, there are multiple priorities from executives and cybersecurity often is not one of them. This type of inconsistency in words and action from executives sends confusing messages to the product teams. For example, one interviewee shared his experience:

"Seeing is believing. At a customer meeting executive talk about cybersecurity being a priority. But you don't see any investment in that area. Bringing it up again shows us they really care. Never bringing it up again makes us wonder if it's really a priority".

Prioritizing cybersecurity in the development process must be done and communicated over multiple channels. Executives, managers, and project owners must have sufficient knowledge about both cyber requirements and available solutions to make good decisions and allocate sufficient resources. For example, managers review and approve reports about the cybersecurity risks within a digital offering, including how the product team handled those risks, before an offering gets to market.

The process for reviewing cyber risks itself is an important mechanism for communicating the urgency and prioritization of cyber features in offerings. The discussions about vulnerabilities, the debates on critical features for offerings, and the communications to customers about cyber risks associated with offerings all indicate how executive prioritize security. The product team learns of their executive's beliefs and attitudes about cybersecurity from these discussions. If the executives do not have background or knowledge to fully engage in these discussions, they will be perceived as "*rubber-stamping the cybersecurity plans*" and the team will also take away the message that cybersecurity is not really a priority.

A more dangerous scenario is when executives don't understand the cybersecurity risks and tradeoffs but act as if they do. Our research found examples where executives were "*book smart but not practical smart*" and are "*dangerously knowledgeable*". Worse still is when the development team believes the uninformed executive's point of view and then focuses on the wrong priority.

Another way the team gets mixed messages is from the performance evaluation and reward system. , When developers are rewarded for elegant designs but not for secure designs, their attitudes will be skewed away from cybersecurity. Many managers voiced similar dichotomies from their organization. Sometimes it was a tradeoff between elegance and security. Other times it was between speed to market and delays due to security vulnerabilities. One manager commented,

"*People feel like their job/bonuses/etc. are tied to when things ship, rather than ship later but better.*"

These managerial mechanisms reinforce perceptions that cybersecurity is secondary to other features and faster delivery. Another interviewee shared the connection with their reward system:

"*We can see how our company prioritizes cybersecurity in who gets recognition. It's not the people who find and fix the cybersecurity issue within products. It's people who come up with new features and products and deliver to customer faster.*",

Though the executives can emphasize the importance of cybersecurity in their digital offerings, the product team will perceive the message through their leader's actions and behaviors. One interviewee summarized this point nicely when they said,

"*Actions and dollars are all that count. Words don't mean anything*."

Action Steps: A Strategy to Bake-In rather than to Bolt-On Cybersecurity

Executives and managers told us that cybersecurity must be built into their offerings, and they seek ways to make this happen. It's no longer something nice to have; it's a necessity. While properly designing for cybersecurity can be both complex and dynamic, bolting-on cybersecurity after the initial design process is not a sustainable strategy either. To sufficiently bake-in cybersecurity, leaders must recognize the challenges discussed above and take action to reduce or eliminate them.

Action #1- Mindset: Find ways to change your developers' mindset so they value cybersecurity and incorporate it into initial designs. Building new products is a team sport, and the team needs to be staffed with the right skills and have the right processes. The SDL process must be part of the initial design process, not bolted-on as an afterthought or as a compliance exercise. Baking cybersecurity into digital offerings needs a process-oriented approach to provide authority and support. Our study identified several practices to make the process more effective, including building a central function that provides common cybersecurity knowledge to the organization, develops a cross-functional group to bridge the knowledge gaps in the team, and provides a cybersecurity champion for each offering.

A central cybersecurity organization facilitates implementation of corporate cybersecurity policies and standards in all offerings. Not every product team comes to their initial offering design meeting with the same level of importance of cybersecurity. But the SDL process with the right managerial support mechanisms can make it easier for the security expertise to be injected into offerings early on.

> "*Unless you have an external organization like us to ensure they are some kind of min security there, there is always some conflict of interest between security and feature for revenue. This is the only way that in our organization that would work*".

Changing the mindset of the design team can be done with a cross-functional team approach where cybersecurity experts are core to the initial design activities. Two relevant comments were:

> "*One thing I saw them do that was very effective was that their exec leadership created a cross-functional team to encourage interactions between teams contributing cybersecurity to that product.*"

Leaders who make changing mindset a priority can do so by encouraging cross-pollination of design and cybersecurity concepts. It sends a strong message of the leader's priority:

> *"Our senior business leader makes the cybersecurity the priority in day one. She reorganizes the team to have at least one cybersecurity representative in each team, driving cybersecurity in each team. Before and after, there is a big change in cybersecurity priority. That sends a clear message saying now cybersecurity is not a joke nor an option, it needs to be taken care of. That helps a lot.*"

The larger community within a company is another source of changing mindset to bake-in cybersecurity. Build a professional community to leverage expertise and reinforce cybersecurity priority. In companies we studied, there were cybersecurity evangelists in unexpected places who together created an influential force.

"*There are 30,000 engineers at our company, and they can do all kinds of things. If they can't do it, they can find other experts to help. They have the budget to hire them. There is nothing they can't do if they are told to do it*."

Having cybersecurity evangelists supports a visible cybersecurity culture and the mindset leaders seek. An internal community is powerful. It can both reinforce the importance of baking in cybersecurity principles from the initial design stages as well as elevate the conversation about cybersecurity to where it becomes a frequent topic of discussion. This also helps promote a culture where people cooperate and work together to build in cybersecurity. As one employee phrased it:

"We are community oriented. People are willing to cooperate and work together to get results. We have no barriers to talk to anyone in the organization about cyber concerns. We are completely transparent."

Action #2- Rewards: Establish visible cybersecurity performance evaluation criteria for the product teams and make heroes out of individuals who display cybersecurity behaviors. What gets measured gets managed. If cybersecurity savvy is not measured as part of performance evaluation, it isn't easy to properly motivate product teams to work towards collective cybersecurity goals. Yet our research showed that the most neglected motivation techniques for cybersecurity behaviors were formal evaluation and reward systems. Find ways to highlight the behaviors you want your developers to do. Reward them for their secure designs. Include security in evaluation processes. Make security metrics public and reward team members for moving them forward.

"Security has become more of a priority for managers because it's more visible at the overall company leadership level. Leaders don't want to be seen not doing cybersecurity. It's part of the regular report to the board. So there is a lot of pain if we don't keep up with that stuff."

For the product team, managers and cybersecurity representatives can make cybersecurity requirements visible throughout the whole development lifecycle. One cybersecurity professional shared a successful story:

"*The cybersecurity representative uses agile workflow, to keep track of the work, create user story based on cybersecurity requirement we need, get cybersecurity piece into the coding schedule, drive it through the process and get the story complete. She asks me to work with her to verify that it is completed comprehensively. She starts it at the very beginning, and I can check it at the end*."

Additionally, when cybersecurity vulnerabilities are uncovered, it's not usually because one individual did something wrong, but because of a series of failures through the organization. Cybersecurity of offerings is a group goal and must be evaluated at the team level. One interviewee explained:

"*If there is a vulnerability, they are not able to release the product. If they are not able to release their product, it means the project will be delayed. It will impact their performance. They will not meet their objective."*

While success building cybersecure offerings is a group goal, individual recognition is impactful, too. One team member commented,

> "*There is a committee to decide who gets to be a corporate expert. I was selected as the cybersecurity corporate expert. This is a big deal for me.* "

There are numerous ways to reward and recognize employees for cybersecurity behaviors. For example, one manager we interviewed shared the value of a financial bonus to an individual who contributed the cybersecurity design to a project. He said that he had given a bonus to someone who solved a complex security project or driven a process that baked cybersecurity into offerings. The same company hands out formal recognition at an annual security conference, in which team members are nominated and recognized for being strong advocates and contributors to security of offerings. Rewards and recognitions can be even as simple as adding a virtual badge to an email signature. By doing so, leaders send a clear message that they value cybersecurity behaviors and are publicly acknowledging it.

Action #3- Messages: Deliver strong messages that increase awareness and drive cybersecure behaviors. One of the most straightforward and widely adopted ways to increase cybersecurity awareness within the organization is to clearly and consistently communicate those goals to all. One interviewee highlighted the impact of constant reminders from executives:

> *"When an executive comes around to do their road show they will speak to cybersecurity in our live events and that tells us that we need to be sure to build cybersecurity into our products".*

Another powerful action was to use marketing to set the standards for behavior. Marketing the offerings as "built with cybersecurity" and using cybersecurity within digital offerings as a selling point by leaders delivers a powerful message that leaders take cybersecurity very seriously.

> *"Leaders often tell our biggest customers and promote our products as 'fastest,' 'lowest cost,' 'best of the breed.' However, lately we heard them say 'it is built with security in mind'. So when marketing speech is about secure products, it trickles down to engineers."*

Designers need to know that customers are increasingly requiring (and valuing) secure offerings. Product teams know that customer requirements are their baseline design criteria. Hence, when customers require cybersecure offerings, design teams will change their behaviors to meet this objective. Make your customer's cybersecurity expectations well-known to design teams. As one product team member told us,

> *"Leaders give us generalities that cybersecurity is important to customers, but engineering likes details. Maybe customers could be invited to come in and talk about it. We like to know the real story. When leaders feel confident enough to bring customers in to talk about cybersecurity, it helps."*

Another strong message comes from how executives handle known cybersecurity vulnerabilities when offerings are ready to be released to the market. When leaders reject products without sufficient

cybersecurity built-in, not only will the product team to find a way to optimize their cybersecurity process, a message is sent that cybersecurity is a priority.

> "*First level managers are coming on much stronger to include cyber security. They realize that if they cannot meet the cybersecurity requirements, they have to ask the execs for a waiver to ship the products. Getting the waiver is much harder, if not impossible, comparing with implementing the necessary cybersecurity requirements. Our general manager won't give a waiver."*

Action #4- Training: Cybersecurity training is necessary but not sufficient and must be supplemented with other managerial activities. The companies we studied, like many organizations, have established cybersecurity training systems to improve cybersecurity awareness and knowledge for employees, but we were surprised that those messages did not transfer easily to offering design. As good citizens of their corporations, product designers regularly commented that they were trained to watch for phishing emails, or to be careful to not click on unknown links. But when asked about design behaviors, these same team members did not list cybersecure designs as something they were trained to do. One senior manager even commented that he just assumed designers knew to make things secure, it didn't dawn on him to explicitly mention it.

Role-dependent cybersecurity training is another way to ensure cybersecurity is baked-in. Organizations can implement baseline cybersecurity training, so everyone understands policies and basic practices. More mature organizations then provide specialized training to help employees across different functions understand their specific use cases for cybersecurity. For example, developers need more cybersecurity knowledge in order to have it permeate their design thinking and incorporate it naturally into their designs and implementation process.

> "*Ideally we train engineers to think cybersecurity on their own. We don't want external person to bring cybersecurity in but conscious thing for teams to think about.*"

Further executives need training too. Security and non-security executives alike would benefit from training on topic such why and how to bake-in, rather than bolt-on, cybersecurity and the importance of constantly modeling the behaviors that show cybersecurity is a priority.

> "*Execs now get that you have to think about cybersecurity from the beginning for new products. They should be done with cybersecurity, rather than retrofit products with patches and updates*".

At the product managers and business designers' level, while they don't need to be knowledgeable enough to implement cybersecurity features, they need to be trained to make the right tradeoffs for cybersecurity. One senior manager emphasized such a urgent need:

> "*We don't have training for product develop managers who make decisions. They don't really understand the tradeoffs about security.*"

Move toward a "baked-in" approach with a cybersecurity culture

Digital offerings are creating new revenue streams for many companies and for every digital offering there are new cybersecurity vulnerabilities that must be addressed. Associating your brand as one with secure offerings is increasingly important. No one wants to see their brand in the headlines like Solar Winds and countless others have seen. Customers expect secure offerings even if they don't explicitly list it as a critical feature. They don't want their company exposed to cybersecurity risk from their vendors.

This research into building more secure offerings highlighted the importance of building a corporate cybersecurity culture that not only keeps your company secure, but that also ingrains the need for reducing cyber risks in products and services your company delivers to the marketplace. Managerial mechanisms such as leaders setting an example and making cybersecurity a priority, performance evaluation systems including evaluation and rewards for cybersecurity actions, and constant and consistent training and awareness campaigns all reinforce the organizational goal of keeping ourselves, our teams, our organization, and our customers secure. Creating a mindset of cybersecurity has ever been more urgent and is at the core of baking-in cybersecurity for our product development processes. One interviewee summed up this concept when they said,

> *"Everyone has a real cybersecurity mentality. We get it because it's engrained in the culture at the highest levels of our organization from day one. It's everywhere in everything you do around here."*

With this mindset, a culture of cybersecurity ensures that everyone has a sense of obligation to "do the right thing". It's this culture that will produce secure products and services that we all expect.