VOICE OF THE COMMUNITY:
CYBERSECURITY

INFORMATION TECHNOLOGY SERVICES

VOICE OF THE COMMUNITY II

Cybersecurity

December 2020

Executive Summary

We think our data is safe until it is not.

Each day, FSU blocks more than 1.7 million email threats and 6,000 web attacks. With cyberthreats constantly evolving and security breaches on the rise, cultivating a cyber-savvy workforce and student population is increasingly vital.

The Cybersecurity Voice of the Community (VOC) study gauges the university's current knowledge of the cyber landscape and best practices in the interest of improving cybersecurity at Florida State University (FSU). Through this effort, Information Technology Services (ITS) identified two foremost issues impeding the adoption of a stronger cybersecurity environment across the university. From these two gaps, four themes emerged as solutions to raising the profile of cybersecurity at FSU.

"You become smart, then they become smarter, and you have to outsmart them again. There's always an opportunity to be better."

Gaps

Two main gaps stand between a stronger cybersecurity environment and FSU. First, there is a desire for more transparency on cybersecurity threats, impact and official university policy. Second, the university community has a hard time grasping the importance of everyone's shared responsibility and the role each person plays to help safeguard our online presence. The root issue is not a lack of observance for cybersecurity but a lack of awareness and understanding of security requirements and their significance in protecting the FSU community.

Solutions

The path forward is clear. FSU needs increased leadership support, expanded training and education and targeted and continual communications to drive a cybersecurity awakening. The four solutions identified are the following.

Unified Effort

The university needs to lead by example and encourage a unified effort to uphold cybersecurity. University leadership must endorse cybersecurity efforts and mandate basic training for all individuals accessing the FSU network. FSU also needs to provide the necessary funding for enhanced training and an ongoing awareness campaign.

Training & Education

FSU needs to incorporate a mandatory training program and ongoing education into university operations. Training should be tailored to audiences and offered in multiple formats. Training must be required as part of new student and employee orientation and frequently revisited throughout one's time at FSU.

Communication

A university-wide awareness campaign is needed to inform and drive people to available cybersecurity resources. Communications should be targeted to each audience and easy to understand. Tangible stories and real-world examples should be coupled with actionable steps and recommended best practices.

Reports & Publication

ITS needs to provide adequate support and clear direction to IT professionals who are resolving cybersecurity vulnerabilities. Advanced training and reporting are needed for highly technical audiences to keep them informed of current cybersecurity concerns and defenses. All communications and education materials need to be stored in an accessible online repository.

Intro

While cybersecurity has been a hot topic for years, the sudden and worldwide shift to virtual operations pushed the matter into the limelight like never before. An increased virtual student population and workforce opens the university to new cybersecurity threats and creates a renewed sense of urgency to educate the university community of those pitfalls better. The Cybersecurity VOC represents a unified effort to reflect on and improve cybersecurity at FSU.

Process

The cybersecurity VOC study took place during Fall 2020. The project team included members from across ITS as well as external stakeholders:

- Kathy Wilkes, User Experience
- Sara Mischler, User Experience
- Tom Doughty, Information Security & Privacy Office
- Cheryl Hester, Office Administration
- Lisa Martin-Brown, Service Management
- Jason Penley, Community Technology Services
- Megan Skowronski, Service Outreach
- Alex Townsend, Research Computing Center
- Katie Townsend, Student Applications Services
- Johnny White, Shared Infrastructure

The study used a combination of focus groups and one-on-one interviews to gather feedback on cybersecurity at FSU and engage stakeholders from across the university. In total, 34 students, faculty and staff participated in the focus groups and interviews.

The cybersecurity VOC was conducted as a follow-up study to the inaugural ITS Voice of the Community campaign conducted during Summer 2019. The original campaign sought to appreciate the current climate towards ITS and understand the expectations of technology used throughout FSU. Following the initial campaign, smaller-scale VOC studies are planned each year to deep dive into specific technology topics of interest.

Gaps

Students, faculty and staff don't know what they don't know about cybersecurity at FSU. The two main gaps impacting the increased adoption of cybersecurity best practices across the university are a desire for transparency and limited understanding of everyone's shared responsibility.

Transparency

The FSU community is looking for greater transparency around university cybersecurity. Students, faculty and staff need a better grasp on the significance of cybersecurity and what they are supposed to be doing or not doing to help keep the university protected. Support for cybersecurity initiatives and policies starts here.

"I'm a firm believer in letting people understand the realities of the challenges that we've had. I mean I have no idea some of the biggest concerns and risk points that for the university."

There is a lack of awareness and understanding of cybersecurity at FSU. Most people don't realize how much university systems are under attack and are interested in hearing the overwhelming numbers and stats. Audiences on campus are not aware of the cybersecurity issues facing the university or the importance of each individual's role in protecting the university from the hazards. Participants said they want to hear tangible stories and real-world examples of how security threats can impact them and the university at large. Students, faculty and staff are looking for specific cases of cybersecurity issues on- and off-campus.

Furthermore, cybersecurity policies exist, but students, faculty and staff either do not know where to find them or do not understand them. As written, policies are hard to follow. It is also unclear who enforces the policies and the penalties for not following them. Policies need to be common knowledge and will hold more value if established as an FSU policy rather than an ITS initiative.

Shared Responsibility

The second cybersecurity gap at FSU is the concept of shared responsibility. It is difficult for individuals to understand how their actions can impact the entire university and why they should care. Efforts to educate the university community are pivotal to establishing a cybersecurity mindset at FSU. We are all part of the problem. We are all part of the solution.

"When we talk about cybersecurity and all those things, for me it's such a difficult topic to look at because it's not tangible. Like it's not something that's actually there."

Basic education is needed on cybersecurity best practices both on- and off-campus. Individuals need a better understanding of the appropriate use of shared devices as well as personal devices and home networks. Faculty members say they need to understand the different classifications of data and resulting security restrictions. What data can be stored in the cloud? Is antivirus software up to date on home computers? What Wi-Fi can be used to sign in to FSU systems? What are the dos and don'ts of flash drives? These are all questions circling the FSU community that need to be addressed and reinforced over time.

The root issue is not a lack of observance for cybersecurity, but a lack of understanding security requirements and their significance. Students, faculty and staff all need more guidance on cybersecurity expectations, potential threats and best practices.

Now that the cybersecurity gaps have been identified, the solutions can be explored.

Solutions

VOC participants identified solutions for addressing the perceived gaps. The following four solutions will help advance the cybersecurity mindset at FSU and ultimately improve the security of FSU individuals and data.

Unified Effort

Establishing a culture of cybersecurity at FSU needs to be a university-wide effort. The university community needs to understand the vital role each of us plays in safeguarding the university, and university leaders must provide the guidance, funding and policies to support the initiative.

> *"For all of us here who are in leadership roles ... being the first ones to take cybersecurity training, participating in these sorts of groups and making time for all the efforts. And so the more people that we have in leadership roles willing to devote time and resources, the more that trickles down and shows this is something that's important."*

The foremost way to uphold cybersecurity at FSU is for university leadership to lead by example. Top-down observance and endorsement of cybersecurity are critical to foster a security-conscious community. University leadership needs to model good behavior and encourage direct reports to do the same. ITS can work with university leadership to get executive support and public backing of large-scale cybersecurity campaigns and training programs. A program should also be developed to support cybersecurity champions in colleges and departments. When university leadership stands behind and endorses the messages ITS sends regarding large-scale security initiatives, it sends a unified response against attacks. Furthermore, leading by example creates a domino effect that elevates the awareness and importance of cybersecurity across the university and reinforces security best practices at all levels of the organization.

To carry out this effort, funding is needed to support cybersecurity initiatives across the university. Allocating dollars to the initiative at the university level signifies the importance of cybersecurity and finances improved and continuous training. Participants suggested that funding can support everything from commissioned training modules to tailored departmental presentations. Funding can also be used to incentivize good cybersecurity practices among students and employees, perhaps through monthly giveaways. Regardless of the delivery method, supporting an ongoing, university-wide cybersecurity program will require a substantial monetary commitment.

The university community also feels strongly that FSU administration needs to mandate cybersecurity training for the entire university. All students, faculty, staff and vendors should be required to undergo regular cybersecurity training, and there should be consequences, such as loss of access to the university network, for those who do not complete the requirements. ITS needs to define implications for non-compliance and get executive backing to enforce the requirements.

"Helping our leadership and those who control our budgets understand eventually the luck is going to run out. The hackers are going to continue to get smarter. And sometimes us getting smarter means that we have to spend a little bit more money to get smarter."

University administration, starting with the president and trickling down to department heads, also need to provide direction on cybersecurity policies and procedures as they relate to individual departments. Existing policies are unknown and difficult to understand. An effort must be made to rewrite security and privacy policies straightforwardly and promote their location in an easily accessible online database. Any potential gaps in security policies, such as requirements when working from home, should be addressed and added to the list of policies.

"They need to keep us in the know on what we need to be doing."

The university community also needs to understand that cybersecurity is everyone's responsibility. This concept is the core of instituting a unified effort to uphold cybersecurity. Every single person at FSU needs to understand the role they play in protecting university data and why their actions matter. Students, faculty and staff want more guidance on cybersecurity best practices and understanding their responsibility both on- and off-campus. Participants specifically requested more direction on the proper use of university-owned and personal devices while working and learning from home. Students, faculty and staff also want to understand better their responsibilities regarding storing university data or documents. Storage solutions differ by role and data type, and data types vary from student contact information to HIPAA-protected records. Individuals need clear direction and training on the measures they should be taking to protect all types of university data. Overall, there is a great desire to support cybersecurity at FSU, but individuals look to central ITS and the university as a whole to guide them toward success.

Training & Education

A strong training and education program forms the cornerstone of an informed and protected university community. Individuals must be educated early and often to understand the critical role they play in upholding cybersecurity both personally and for the entire university. The FSU community is eager for more cybersecurity training, and it is the responsibility of ITS to deliver.

Across the board, students, faculty and staff all emphasized the importance of implementing mandatory cybersecurity training at FSU. Multiple tiers of training tailored to affiliations, roles and organizations are needed, and training could extend beyond the internal FSU community to vendors and guests. A dynamic cybersecurity training module should be added to student orientation and employee onboarding, and completion of an introductory cybersecurity course should be a required step for anyone accessing the university network. In addition, cybersecurity training should be a requirement for the creation of a student registered service organization. Anyone interacting with university digital resources needs to be informed on proper cybersecurity etiquette and rules.

Beyond mandatory introductory training, training needs to be a continual and constant process for all FSU. Students recommend regularly presenting cybersecurity training for all fraternity and sorority life organizations, freshman interest groups and other prevalent student groups such as the Student Government Association. Students also feel cybersecurity expectations should be included in course honor codes. On the employee side, faculty and staff should be required to complete regular security refresher courses to help them stay abreast of the changing cybersecurity landscape. These consistent education efforts will make cybersecurity become a learned behavior.

Audiences tend to have a natural resistance to security changes at FSU, whether it's staff members who don't like using a personal device for work purposes or faculty who feel it now requires more steps to get their job done. However, proper training and education on new security requirements and practices before they roll out would help lessen opposition and smooth the transition. Early notice and positive reinforcement about the importance of new security measures can promote a more willing and agreeable adoption.

"This is important in any new technology implementation. [Making] it clear and easy to understand the instructions from day zero for your consumers will ease that adoption path dramatically."

Requested topics for cybersecurity training are vast. Participants expressed interest in cybersecurity training for everything from specific applications, such as Outlook and Excel, to particular tasks, such as password resets. A cybersecurity element should be incorporated into basic training for all university applications and software. For example, training guides and documents similar to the *10 Ways to Secure Zoom Meetings* infographic should be developed and shared for all new technical services at FSU. Multiple requests were made for education on password best practices. Staff and IT professionals also requested training on security policies and considerations for new third-party contracts that are brokered through FSU.

Training should be offered in multiple formats to meet different learning styles. Face-to-face training, whether in-person or via Zoom, is desirable to all audiences. Online training can also be very impactful; participants specifically referenced the mental health first aid training coordinated by Human Resources in Fall 2020. Video training has potential but needs to excite

viewers in the first few seconds to capture one's attention and be effective. Regardless of the forum, it is essential that training is engaging and interactive.

Communication

"We don't know what we don't know." Currently, the FSU community is not aware of what cybersecurity resources are available. To drive cybersecurity home, the FSU community needs—and wants—continuing communication about current threats and the protections they should take.

A large-scale awareness campaign is needed to inform and propel people to available cybersecurity resources. Once a suite of useful training materials is developed, a university-wide awareness campaign should be launched to encourage the use of the online resources. After the initial push, regular communications should promote cybersecurity best practices and remind individuals of the information.

" We need to keep it in their face as much as we can. Not necessarily to inundate them with more information, but to share the importance of protecting our data."

Effective communications use the platforms FSU audiences visit most frequently and provide targeted and timely information. Participants suggested placing important security information directly on the FSU homepage (fsu.edu) and other frequented online locations such as myFSU Portal. Beyond mass communication channels, the key is targeting the delivery to the audience. Faculty prefer targeted emails, while social media is an excellent place to educate students.

The type of information to be shared is varied. Individuals are interested in receiving alerts and solutions to current cyberthreats as well as information on university cybersecurity initiatives and projects overall. Specific topical requests include password best practices, shared devices and university security policies. Staff specifically requested communications about 2FA workarounds and alternate ways to verify their identity when their cellphone is not available. Faculty would like a greater understanding of university policies regarding intellectual property. IT professionals and staff with purchasing responsibilities are interested in understanding cloud storage contracts and what data can be stored in third-party applications. Regardless of the topic, each source should provide at-a-glance information and tips and link to in-depth resources stored on the ITS website for those who want to learn more on specific topics.

"I think cybersecurity needs to be normalized in a way where we are so familiar with it and it's such a habit that it's not something that we dread or that we have to fight against or struggle with."

On a related topic, many students, faculty and staff use various online tools to communicate and collaborate with colleagues, with Dropbox and Google Workspace leading the pack. Individuals gravitate toward these tools for their ease of use, large user base and free access. However, people remain concerned about these tools' security when sharing and transferring classified research data and other content. As such, there is a strong desire for FSU to provide educational licenses with advanced security controls for such tools. Since they are already being used unofficially, faculty and researchers feel strongly that university contracts with popular collaboration tools would close a potential security hole. This would give the FSU community the solutions they need to securely transfer data electronically both within FSU and across the globe. If ITS chooses not to support additional collaboration tools, communication is needed explaining why FSU uses the tools it does and why those decisions were made.

“One of the biggest gaps that FSU has is FSU provides the services they want to provide and doesn’t engage in the services that are being requested.”

Communications must be easy to understand and clearly state how to take action. Messages need to avoid "tech speak" and instead explain security concerns and recommendations in a way that is easy to follow for everyone. Messages should clearly and concisely outline a problem and provide action steps toward a solution. Possible approaches include publishing monthly tips highlighting cybersecurity best practices or biggest threats and creating a series of checklists for cybersecurity in different scenarios, such as working from home or purchasing a new cellphone.

"People don’t necessarily know what’s out there ... They get one look at it, and it’s just a confusing block of stuff that doesn’t translate to the way our brains interpret things."

Most importantly, communications need to be transparent. Cybersecurity can be an abstract subject for some people. Real-world examples targeted to the audience can make the message clearer. Communications should share real stories of real issues—paychecks redirected and student financial aid funds stolen—that have happened to FSU students and employees. Audience-specific examples of cyberthreats should be included in marketing campaigns as well as training materials. Individuals also want to know statistics on how often attempts are made against FSU environments. Sharing the mind-boggling numbers of how many spam emails are blocked every day and attacks blocked by university firewalls will help to tell the story of why FSU needs this level of security. Tangible and transparent stories make messages relatable and drive action.

Reports & Publication

ITS is obligated to provide IT professionals with the resources and support they need to protect the university's digital infrastructure adequately. We ensure protection for FSU when IT professionals—the people on the frontlines maintaining the university's technology—feel central ITS is supporting them and everyone is working cohesively across the university.

When vulnerabilities are detected in an FSU system, careful direction and guidance are necessary for the impacted university unit. Often, university units find Nexpose and InsightVM vulnerability reports hard to follow and receive little assistance from ITS to remediate known issues. ITS must take an "in-it-together" approach and provide clear instructions and one-on-one support when needed to resolve common vulnerabilities. All related communications must be straightforward and free of technical jargon with actionable steps to fix the issues.

"FSU pretends that ISPO or ITS does their job informing us about vulnerabilities, but nobody trains us or works with us on how to address them, and we don't have enough expertise to deal with it."

Advanced training is also required for university technical audiences. In-depth training on interpreting vulnerability and other security reports will make the documents easier to understand. In addition, optional training on fixing common security issues would be helpful, especially for individuals who have been assigned IT responsibilities as "other duties as assigned." Monthly reports on the most significant threats facing higher education and recommendations for common bug fixes can help keep cybersecurity a priority among IT professionals across FSU. The better we can educate the university's distributed IT population on common vulnerabilities and best practices for preventing or resolving security issues, the better we can protect the university.

IT professionals also suggested creating an easy-to-access online repository of all cybersecurity training and education materials. This one-stop-shop would include security-related presentations, PDFs and hyperlinks in a single location, saving individuals from having to recall past communications or search for attachments and links in old emails. The website-based storehouse would organize materials by topic and could include everything from links sent in emails to documents shared in meetings to publications referenced by the industry. This resource can also be expanded to all students, faculty and staff.

"It would be better for me if all of the training material was all stored in one place. That way I can refer people to it or if I need to get the file I know where to get it."

Conclusion

Overall, participants said there is a lack of awareness and limited organized effort to encourage cybersecurity at FSU. The good news is the FSU community says they want to learn.

ITS can build a strong cybersecurity environment at FSU by being more transparent with security requirements and the rationale and highlighting the shared responsibility everyone has to uphold cybersecurity at FSU.

"I think it's not only good practice to be a good cybercitizen but also a good preparation for the future ahead of you."

Progress starts with a top-down approach and a unified effort to model acceptable cybersecurity practices and mandate basic cybersecurity training for the entire FSU community. Training needs to be tailored to specific roles and organizations and should be offered continually to share current best practices and keep cybersecurity top of mind. A large-scale awareness campaign and regular communications are needed to promote training requirements and share available resources to encourage adoption. All of these resources need to be organized in an easy-to-find online location, and ITS must take a more active support role in providing one-on-one support as is necessary to IT professionals and others on the cybersecurity frontlines.

"It's a never-ending process, and it's exhausting to think about. But it's what we have to do."

Working together with the university community, ITS can lead a significant and vital shift in cybersecurity awareness and compliance at FSU. With these recommendations, the campus will be safer from cyberthreats and more unified in our effort to educate and promote healthy online habits.