

# Information Security Through a Community of Practice: Tom Sawyer's Approach

*A community of practice helped West Point achieve dual goals: a secure network, and graduates and faculty who understand information security*

By **Donald J. Welch**

The United States Military Academy (USMA) at West Point is both an academic institution and a military post. As such, it must maintain the free access to information expected of higher education while meeting military security standards. Because successful security requires out-thinking potential adversaries, it is a challenging task in its own right. When the IT support staff and the faculty do not understand each other's perspectives, however, it is impossible.

*"I had to block that port at the firewall—the latest worm uses it."*

—Network Manager

*"You shut down my lab without any warning!"*

—Professor

Sound familiar? This exchange typifies the conversation between faculty and network administrators in years past. Balancing security and access is never easy, especially at academic institutions that prize creativity, individualism, and open access to information. It was especially difficult in our case, because neither network administrators nor faculty felt that their perspective was truly understood.

At West Point we addressed both concerns by forming a computer security community of practice that includes



## Forgot your password?

both faculty and staff members. The community of practice has increased West Point's collective knowledge of information security, and the members have come to respect and understand each other's points of view. The results are a shared sense of ownership of network security and a much improved security posture, without degrading the usefulness of the network.

### Background

The damage caused by computer network attacks<sup>1</sup> and pressure from the government<sup>2</sup> are causing most academic institutions to consider security in their network operations. West Point is part of the Department of Defense (DoD), so it must comply with DoD and U.S. Army security standards and policy. Because of this we might be ahead of many schools in placing a priority on securing our network, but this won't be the case for long.

Many factors make information security difficult. First, the adversary is always a thinking, willful, and creative human aided by the formidable technical tools a computer can provide. This makes the field very dynamic. As soon as defenders develop a counter, attackers are at work on a way to defeat it. The old saying, "A chain is only as strong as its weakest link," was never more true than as a metaphor for network security. If there is a way past the network defense, attackers will find it and exploit it.

Second, the network at a university is indispensable to teaching and learning. The wrong security measures can be more effective than even a skilled attacker at denying legitimate users access to the network resources. Deciding how much risk to take, understanding the full ramifications of a security measure, keeping administrators and users educated and vigilant—all are very difficult tasks for IT leaders.

## The Problem

Institutions of higher education, like every presence in cyberspace, face an increased threat of attack. The damage done is significant and can harm an institution's ability to perform its educational mission effectively. Mounting an effective defense has two critical components: developing the best solution and garnering the support of the user community.

Security is not a state but a process. An institution must accomplish its mission while maintaining an acceptable level of risk. Determining an acceptable level of risk is difficult because the factors involved are many and complex. Simply put, how do educational institutions develop architectures, policies, and user education that strike the proper balance while gaining the support of all involved?

Faculty tend to raise a proverbial eyebrow at any restrictions that network administrators place on the network. Security measures that restrict the use of the institutional network often meet with resistance that can cross into defiance. An acceptable level of security cannot be achieved by fiat. For a defense to be effective, network users must not circumvent security measures. They also must comply with security policies and, ideally, participate in the network's defense. How can administrators evoke cooperation, and even a sense of ownership of computer network security, from the faculty?

## Previous Attempts

Military networks must undergo a security audit to operate. West Point had been operating under a waiver from the Army because we could not comply with the security standards and maintain the network as the viable, education tool we had come to rely on. Network administrators and managers gained most of their experience with the field Army, where the philosophy is to deny access to information unless there was a need—security was the priority. They saw many of the faculty complaints as not relevant because security always trumped functionality from their perspective.

The faculty, many of whom were Army officers, thought of the network in academic terms. They felt that access

## An institution must accomplish its mission while maintaining an acceptable level of risk.

and functionality should only be denied for very good reasons. Inquisitiveness, creativity, and exploration should not only be allowed but fostered. From the faculty perspective, a professor should be allowed to install and experiment with a shareware program that might add to the value of a class. Administrators should not only allow this but help the process along.

Animosity grew. At the same time, it became very difficult for the academy to make any major changes to the network. Many on campus believed that the key to solving the impasse was communication. The senior leadership held meetings to discuss major decisions, but the results were disappointing.

The normal course of a decision went like this: Both sides stated their initial positions, each hardened its position, and the resulting decision left one or both sides feeling wronged. Even though a decision had been made, implementation was problematic because support on campus was uneven. As individuals implemented the decisions, they made interpretations or cooperated based on their own beliefs. Leaders might tacitly support users who waded into gray areas because they did not agree with the decision in the first place. This deadlock left us constantly struggling—and without satisfactory security.

## The Solution: Establishing a Community of Practice

Graduates and faculty must go to the Army intellectually better off than when they arrived at West Point. More computer security knowledge is something that everybody values. Using knowledge as lucre, we give everybody something of value and develop cooperation.

Our institutional goals with respect

to computer security are twofold. One goal is a secure and robust network that is an integral part of West Point's learning infrastructure. The other is to develop educated leaders who understand information security.

We can accomplish both institutional goals through a community of practice. Communities of practice, according to Wenger, McDermott, and Snyder, "are groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in the area by interacting on an ongoing basis."<sup>3</sup> They don't just share abstract knowledge; they work to solve real problems. In a well-operating community of practice, knowledge is shared, mentoring occurs, and actual problems are solved. All members find value from the interactions, whether they learn, teach, solve problems, or find solutions to their toughest problems. They are members because they believe they benefit from their participation.

Communities of practice lie outside the normal organization of an institution. Members are not assigned positions by management; they gain their authority from the consensus of the members themselves. They bring value to the community based on their perspectives from their positions in the organization, but the key is their knowledge. In a successful community of practice, knowledge is what counts—sharing it, gaining it, and applying it.

We established the West Point Computer Emergency Response Team (CERT) with two goals in mind. We wanted

- the best possible solutions, and
- a sense of ownership of network security from all groups at the USMA.

The problems the CERT solves are of two types. First, the CERT responds to ongoing network attacks quickly and appropriately. It is the medium through which the best computer security minds at West Point identify attacks and think through responses. Second, the CERT develops the security architecture, policy, and training packages for the West Point computer network through the chief information officer. Even though the CERT has no formal power, its recommendations are taken very seriously.

## **Community Characteristics**

The West Point CERT is a community of practice rather than a committee. People join and stay in communities of practice because they find value in the interactions.<sup>4</sup> Knowledge is the coin of the realm at a university, and the best way to attract faculty is to offer opportunities for learning and teaching.

The IT field is also a knowledge-intensive field, so the opportunity to learn is a strong enticement to the IT support staff, too. Many people at the USMA have expertise in computer network security. The Department of Electrical Engineering and Computer Science has a center focused on computer network security research. They bring familiarity with and understanding of the current computer security literature to the CERT. Experienced system administrators bring years of experience securing networks, especially the West Point network, to the CERT. Additionally, Army officers who have worked computer network security in other Army assignments bring that experience to the CERT. All members have something to contribute, and all have something to learn.

The CERT is not just for sharing knowledge among peers; it also develops junior members. Because West Point has a high proportion of active duty Army personnel on the staff and faculty, turnover is high. New people not only must become familiar with our environment quickly, they must develop their skills to secure the West Point network and bring that knowledge back out to the Army. The CERT serves a valuable function in this way, too.

CERT membership is by consensus. Anyone can attend a meeting or join the e-mail list. The typical progression to membership starts with someone suggesting attending CERT meetings to a colleague. The person normally attends first as a lurker—sitting in the back of the room and listening. Many people are intimidated at first and reluctant to offer comments. After a while, some realize that they can contribute and will speak up during a discussion. Usually, they start by asking questions, and then begin to offer answers. The CERT values their attendance, so they are members by consensus.

Some people continue to lurk, never contributing but finding enough value to justify attending meetings. Others find higher priority things to do than go to a CERT meeting. As their attendance gets more sporadic, the quality of their participation usually drops.

Anyone can bring up a problem or offer an opinion. The group reaction to the input provides feedback on the quality. Participants are polite, but a comment that is ignored by the group gives the originator all the feedback needed. This informal process works very well.

We have found that CERT meetings also “right-size” themselves. Too many people, and the value of the meetings goes down. As a result, we lose some people. With too few people attending, we skip a week unless we have a hot topic. CERT meetings average about 20 people. The CERT e-mail list currently has 37 names, but a core of about 12 people always attends. For perspective, West Point has about 200 IT workers and around 50 faculty of computer-related disciplines.

The CERT also disciplines itself with respect to its agenda. If the discussion veers away from security, a member will point out that the topic is best solved in a different forum. Even a senior member of the CERT who brings up a problem not interesting to the other attendees will find the topic met by a deafening silence. Because CERT membership is voluntary, members only participate if they get something from attending. Developing the proper language for a policy might be important, but CERT members find addressing the problem that motivates the policy much more fun.

## **Community Operations**

Because the West Point CERT is not a committee and exists outside the IT support structure, it operates in a very informal manner. Although I originally organized the CERT and happen to hold a senior position at West Point, I am not in a position of authority over most of the CERT members. My influence in the CERT, like any other member's, is based on my knowledge and experience. The CIO's office disseminates the time, place,

and proposed agenda for meetings and provides official status for the CERT, but does not control the group's activities. The group decides the actual agenda the day before, by e-mail.

CERT members work together to make decisions that affect the entire campus, but many departments or smaller organizations also make decisions that ostensibly affect only their area but in reality affect the entire network. The knowledge shared in the CERT raises the quality of these localized decisions, making the entire network stronger.

In coming up with a policy recommendation, the CERT acts as a consultant to the CIO. Take the example of the policy on peer-to-peer (P2P) programs on the network. This complex issue crosses many boundaries and, in the past, certainly would have fostered animosity and mistrust. The CERT was concerned because of the security implications. We discussed the appropriate uses of P2P and the future of P2P in both academic and mainstream computing, along with the vulnerabilities that P2P introduces to a network and ways in which we could mitigate those vulnerabilities. After much discussion, both in-person and through e-mail, the CERT recommended that we ban all P2P file-sharing software based on the security threat, leaving aside the legal and ethical considerations of the files being shared. We also acknowledged that this will probably be a short-lived policy, as P2P becomes more common in legitimate applications.

The CIO turned this recommendation into a policy letter and presented it to the CERT for comment. He was not bound by the recommendation, nor was he obliged to show the policy to the CERT before acting on it. The results were a much better policy than West Point could have developed without the CERT and emissaries who explained and promoted the policy to the faculty.

The CERT has its own e-mail list, which, in case of an emergency, is usually the first place an issue is raised. If the situation demands it, available members will meet to deal with the problem. Because e-mail is sometimes not available during an attack, CERT members also share home and cellular phone

numbers as well as e-mail addresses outside the West Point network.

The CERT meets once a week. The discussions sometimes result in a product, such as the West Point security architecture, or a recommendation to the West Point leadership, such as a policy. Sometimes the group provides a solution to a problem raised by a CERT member, who is free to take that solution and implement it.

Because the CERT members not only share knowledge but gain perspective from each other, the meetings are central to the group's effectiveness. Many communities of practice can operate almost or entirely virtually. One of the keys to our success has been the personal relationships that have developed through the CERT.

### **Community Influence**

The CERT's influence is felt widely but rarely directly. The CERT member who brings a problem to the group brings back a better understanding of how to solve the problem or even a solution that worked somewhere else. The CIO is not required to follow any recommendations of the CERT; however, he has never ignored the CERT's recommendations. He knows that the CERT does the best job of developing the right answer with respect to security of any entity at West Point. He also knows that once the CERT settles on a position, he will have a network of experts who support the decision throughout the campus.

As a result of the CERT, the West Point IT community knows more about security, sees the many perspectives of security, and feels a sense of ownership of network security at West Point. Faculty have pointed out security problems, knowing potential solutions could negatively affect the education mission, and then applied their abilities to finding workable solutions. Because of their involvement, faculty were much more accepting of restrictions. They understood the requirements and helped determine that there were no other workable alternatives.

Faculty involved in the CERT are mostly computer scientists, but their

influence on the rest of the faculty is profound. They defend the decisions to their peers, and because of their status the rest of the faculty trust them.

The IT support personnel, who focus on the network's operation, are more cognizant than faculty of current Army policy and the practical difficulties in network security. On the other hand, they now have a much better understanding of how to support teaching and learning with IT. They also have a much better understanding of the state-of-the-art in network security, thanks to the CERT. Faculty, administrators, and managers have all learned to trust the CERT recommendations.

### **Results**

USMA has had two external security assessments and one internal assessment since the formation of the CERT. West Point not only met the standards but was found to have a better security posture than most of the Army installations that have undergone similar assessments. These results are even more remarkable when the 4,000 student-owned computers are considered, as well as our greater need for open access to information compared to other Army posts. One member of the assessment team who had inspected West Point prior to the CERT said he was astounded by the change in the year since his last visit.


Since the creation of the West Point CERT, no major attack against our network has succeeded. In the past West Point suffered serious damage from the Melissa and ILOVEYOU viruses. Code Red and Nimda passed us relatively harmlessly. Like most, we suffered through the denial of service associated with the SQL Slammer worm, but we were back up to full capability fairly quickly after the worst of the storm passed. Individual hosts have been successfully attacked, but the damage has been slight and the attack contained before it could spread.

The West Point CERT still meets weekly. We reexamine decisions as necessary. As previously stated, security is not a state but a process. Every major security decision at West Point is first

analyzed by the CERT, whose members are experts and know the environment. The CERT passes on recommendations to the CIO to turn into policy or implement otherwise.

### **Conclusions**

To implement an effective information security program at West Point, we had to overcome two problems: we had to get everybody, especially the faculty, to support the program, and we had to better understand information security. CERT recommendations have succeeded because of their high quality and because faculty were involved, making for better acceptance on campus. The CERT itself is a success because members continue to feel rewarded for their membership. Members learn and bring the knowledge back to their organizations, so West Point as a whole knows more about security and has a more secure network.

Information security is difficult, and all users must participate. Getting the faculty to buy in to security is tough. As Tom Sawyer figured out, if you can get people interested in what you do, they might take your task as their own and have fun doing it. Communities of practice are a great way for organizations to share and thus increase knowledge. In an institution devoted to teaching and learning, participating in a community of practice can be even more fun than whitewashing a fence. 

### **Endnotes**

1. F. Olsen, "The Growing Vulnerability of Campus Networks," *The Chronicle of Higher Education*, March 15, 2002.
2. D. Carnevale, "Presidential Panel Calls on Colleges to Aid in Security Networks," *The Chronicle of Higher Education*, October 4, 2002.
3. E. Wenger, R. McDermott, and W. Snyder, *Cultivating Communities of Practice* (Boston: Harvard Business School Press, 2002).
4. Ibid.

---

Colonel Donald J. Welch ([welch@usma.edu](mailto:welch@usma.edu)) is Associate Dean for Information and Educational Technology at the United States Military Academy at West Point, New York.