Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Using Teambuilding to Improve Performance for Geographically Distributed Information Security Professionals

IT Security agents are often distributed geographically. Many team building techniques focus on groups who can gather physically and can do offsite activities together. IT Security collectives can improve their ability to work together if they engage in team building activities which can be done virtually. This paper describes the change in leader opinions as a result of team building activities conducted in working groups that were geographically disbursed. It also documents some objective measures of security which w...

Copyright SANS Institute

Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Using Teambuilding to Improve Performance for Geographically Distributed Information Security Professionals

GIAC (GSLC) Gold Certification

Author: Julie A. Kent, Julie_A_Kent@raytheon.com
Advisor: Kees Leune

Accepted: December 2012

Abstract

IT Security agents are often distributed geographically. Many team building techniques focus on groups who can gather physically and can do offsite activities together. IT Security collectives can improve their ability to work together if they engage in team building activities which can be done virtually. This paper describes the change in leader opinions as a result of team building activities conducted in working groups that were geographically disbursed. It also documents some objective measures of security which were positively impacted by focusing on team interaction.

1. Introduction

In recent years there has been a focus on work being done in teams rather than individually. This may be because multiple minds can generate better ideas, but it may also be due to the complex nature of work or the quantity of work which must be performed (Bossche, Gijselaers, Segers, Woltjer, & Kirschner, 2010). Securing information technology (IT) for large networked organizations is a complex task which takes place in multiple locations. The task is complex because practitioners must understand the goals of the organization, how the organization plans to use IT to further those goals, the threats to the organization, the threats to the IT systems, the vulnerabilities of the IT systems, and how to reinforce the vulnerabilities in order to mitigate the threats. Since technology changes rapidly, IT security practitioners must spend significant time and energy keeping knowledge and skills up to date with changing technology.

1.1. Using Teams to Secure Information Systems

With the advent of networked organizations the vulnerabilities in IT security increased exponentially over the vulnerabilities of standalone systems (Gupta, Banerjee, Agrawal, & Rao, 2008). This made it sensible to start employing IT security professionals in teams each concentrating on vulnerabilities in specific parts of the IT system. As networks expanded from local area networks to campus wide systems and then to the internet, many organizations discovered they had IT security issues that were physically separated from the teams with the knowledge to address those issues (Assel, Wesner, & Kipp, 2009). In some cases organizations decided to break up the team and have different members located near specific locations. In other cases, organizations co-opted IT staff who were supporting new locations from a technology view to include security aspects (Assel et al., 2009). In either case, the result was a group of people looking at security issues who were not able to regularly meet face to face.

1.2. Challenges of Distributed Teams

Teams which are collocated may use all types of communication including face to face, shared physical diagrams and pictures, telephone, email, and instant messaging. Teams which are geographically dispersed have a higher cost to communication and the mechanisms available are more limited (Espinosa, Slaughter, Kraut, & Herbsleb, 2007). Geographically distributed teams must pay attention to more factors in order to interact successfully. This includes scheduling teleconferences when parties across multiple time zones are available, working through different holiday schedules and work customs and perhaps even addressing different primary languages. Table 1 summarizes some of the challenges faced by these teams.

Table 1 - Challenges Facing Geographically Dispersed Network Security Teams

Challenge	Possible Causes
Remote team mates slower to respond to network security alerts	Delay in notification Challenges knowing or accessing the appropriate response Time zone differences resulting in different working hours
Individuals may be unaware of business activity in other areas that affect network activity patterns	Insufficient attention to business activity as opposed to technology Lack of effective communication
Network equipment at some sites may have less capability than at other sites	Different refresh rates Different needs based on site size and activity International customs and sales restrictions
Users at remote locations may not understand security policy	Lack of effective communication Different language and culture resulting in different interpretations of policy

One specific security related question is how to verify identity and coordinate activity for teams that are geographically separate. Physically collocated teams generally use verbal observation to verify identity. At initial introduction this may mean comparing a face to an employment badge, but it may also be verified through introduction by a trusted third party such as a human resources representative or a manager. Geographically dispersed teams have more of a challenge in verifying identity(Aubert & Kelsey, 2003). Depending on the sensitivity of the information being discussed, teams may settle for knowledge of the conference call number and individual verbal introduction as sufficient. In other circumstances, teams may go through the effort of setting up a teleconference in order to have visual verification of identity. They may put

a pass code on a voice only call. They may create a chat room which is only open to invited members and then distribute information for a verbal call in the chat room. Teams may set up multi-factor authentication for their online meetings. All of these mechanisms take more time and are more cumbersome than gathering in a meeting room. Thus, more overhead is required for geographically dispersed teams to carry on team activity.

The overhead burden is even more challenging when it relates to security issues. Often ideas concerning security need to be shared with team mates rapidly either due to an emerging vulnerability or an immediate threat. The delay required to set up a virtual meeting versus setting up a physical meeting can make it more difficult for the virtual team to complete their job. However, since the security situation may change at any time, specifically it may change when a collocated team is not in their normal working environment; the geographically dispersed team may at times have an advantage. Since they are used to working in a dispersed mode, they do not have to gather at a particular location to begin responding to a crisis.

1.3. Improving Team Abilities

Team building, consciously looking at ways to work better together, can improve team communication and coordination. The resulting team can work together more effectively thereby overcoming the difficulties of geographic dispersion (Fiore, Salas, Cuevas, & Bowers, 2003) and can improve network security and data security. Team building can also foster trust between members; trust in each other's skills and in the ability of the team to work toward mission goals. Trust is essential to building an effective team in a distributed networked environment(Mezgár, 2003).

Network security requires the ability to work together to implement security controls. It also requires the ability to coordinate activity in response to security breaches and in response to the discovery of new vulnerabilities. Teams may have explicit or implicit ways of coordinating their activities (Espinosa, Lerch, & Kraut, 2009).

Team building activities have been shown to improve the effectiveness of teams(Bossche et al., 2010). Different activities are useful depending on the length of time the team has been

working together. Teams generally go through the stages of forming, storming, norming, performing, and perhaps mourning(Staggers, Garcia, & Nagelhout, 2008). Activities are designed to support the team in each of these stages. However, investigation of these activities shows that most of them were designed for teams that have the ability to meet in a face to face setting(Staggers et al., 2008). While these can be very effective in improving the effectiveness of teams who have the advantage of meeting face to face, there is significant cost involved in bringing together geographically dispersed IT security teams. In addition, due to the rapid response required for many IT security tasks, teams may be formed on the fly without any opportunity to meet face to face before commencing work.

2. Case Study of Small Work Teams in Information Technology

In this case study an Information Technology unit was divided into three teams each responsible for different aspects of system operations including information security. Each team was responsible for working with appropriate counterparts in a large corporation who were not co-located. In one team all members of the local group worked primarily in the same physical location. The second group included several remote individuals while the third group consisted entirely of individuals who worked at locations remote from the team lead and each other. At the beginning of the case study a survey of the team leads was taken to indicate the cohesiveness of their teams. The team leads used an “Assessment of Virtual Teams” to evaluate the effectiveness of their teams (Guillot, 2002).

The team leaders were then given training in specific team building exercises to consider conducting with their teams. To encourage the formation of team identity, teams were expected to review progress toward annual goals. The goals included taking objective measures of team performance. Teams were expected to set up regular meetings to discuss progress towards these goals. Team leaders were expected to actively engage in team building for their teams. After two months, the team leaders were then reassessed using the same survey.

2.1. Team Building Activities

The teams were challenged at finding team building activities that could be done without being collocated. There are many useful sources of team building activities such as (Sugar & Takacs, 2000) or (Thiagarajan & Parker, 1999), but most of them expect the team to be gathered in the same location. Existing activities that could be modified to produce an online activity were discussed. The team leaders then participated in a team building exercise themselves to improve their ability to work as a cohesive unit. This involved working an online scavenger hunt on the corporate Intranet without using verbal communication. Limiting communication in this manner helped the team leads to practice operating as if they were not collocated. It also gave them an exercise which they could use with their respective teams.

Each team lead succeeded in finding at least one specific team building activity which could be done with their unique group. In general, this involved modifying an activity by customizing it for their unique situation(Staggers et al., 2008). Since these activities were not directly related to the work performed they may not have assisted the teams in building a shared mental model of their situations(Resick, Dickson, Mitchelson, Allison, & Clark, 2010). However, they did allow the teams to come to know one another better and to learn what to expect from one another(Espevik, Johnsen, & Eid, 2011). This may have contributed to the overall increase in effectiveness of the teams.

3. Results

Results include both the responses to the assessments and real world performance indicators. The actual survey results are given in the appendix. A chart showing the differences between the beginning and the end of the period is shown below in Figure 1.

Figure - *Change in Team Cohesion Over Two Months*

It was interesting to note that there are several places where the assessment results went down. This may be the result of personal sentiment at the moment the assessment was performed. However, it may indicate team leads who have learned more about particular

behaviors have higher expectations and therefore judge their own team more critically. It should be noted that all of the teams experienced a change in personnel during the relatively short time of the study. In addition, since this occurred in a real work environment, there were vacations, personal leave, bereavement leave, and other events which gave individuals reasons to put their personal situations ahead of the needs of the team.

Not surprisingly the team which was able to meet for a face to face collaboration session showed the most improvement in their virtual team assessment. This indicates that even groups who are skilled in working without the benefit of face to face contact can gain improvements from meeting as a group.

3.1. Real world performance indicators

The teams in this case study are engaged in supporting a variety of computer systems performing asset management, contract support, and financial tracking for a large defense contractor. As such, the teams were interested in measurable improvements that could be reported to company management. Results are tracked from the point of view of application security, individual host security, and incident reporting.

The most notable improvement came in the area of application security. Application vulnerability scans are conducted annually and after major application upgrades. The scans performed prior to training took weeks to resolve with corporate IA. There were prolonged email threads concerning how to mitigate certain results along with numerous teleconferences and individual phone calls. Similar scans, conducted after training, were resolved in one 30 minute meeting. The work the team did to increase their ability to work together appears to have improved their ability to communicate with other organizations outside the team.

Host based vulnerability scans are run by another corporate organization and reported weekly. On these scans 0 is a perfect score indicating no known vulnerabilities, but many systems run with consistent known low vulnerabilities because the vulnerabilities are inherent in the system function. The team involved in this study was working to reduce their high scores on these scans. They successfully reduced the high score by 30%. They were not

tracking their average score. Examining the data after the fact it was determined that the average scores actually increased by almost 25%. However, both the high scores and the average scores for the team engaged in teambuilding were an order of magnitude lower than for a similar team which was not engaged in teambuilding.

Security incidents were generally infractions of policy and reported from automated tools that monitored user activity. The number of security incidents reported went from 4 per week at the beginning of the period to 3 per week at the end of the period. The decrease in incidents may be the result of improved communication from this team. Length of time to respond and resolve a security incident remained the same at approximately 3 days from the time the incident was detected until it was resolved.

The teams were not initially comfortable with the idea of finding objective measures of team performance. The team leads were used to having objective measures which focused on individual performance. Through discussion, the team goals were turned into project plans which were tracked during the period of the case study. The project plans and current project status served as another objective measure of team performance. Turning goals into projects improved the reliability of status reports on goal achievement, but did not necessarily improve the speed with which the goals were reached.

4. Conclusions

There needs to be more research done on the best ways for geographically dispersed teams to operate over time. There is a tendency in industry to assume teams need to be collocated in order to gain the synergies that come from working together. This has resulted in increased expense for travel and for relocation. Improving our ability to work across distance may save time and money. Due to the distributed nature of security work, improving the ability of security teams to work across distance will result in a more secure enterprise.

5. References

Assel, Matthias, Wesner, Stefan, & Kipp, Alexander. (2009). A security framework for dynamic collaborative working environments. *Identity in the Information Society, 2*(2), 171-187. doi: 10.1007/s12394-009-0027-1

Aubert, Benoit A., & Kelsey, Barbara L. (2003). Further Understanding of Trust and Performance in Virtual Teams. *Small Group Research, 34*(5), 575-618. doi: 10.1177/1046496403256011

Bossche, Piet, Gijselaers, Wim, Segers, Mien, Woltjer, Geert, & Kirschner, Paul. (2010). Team learning: building shared mental models. *Instructional Science, 39*(3), 283-301. doi: 10.1007/s11251-010-9128-3

Espevik, Roar, Johnsen, Bjørn Helge, & Eid, Jarle. (2011). Communication and Performance in Co-Located and Distributed Teams: An Issue of Shared Mental Models of Team Members? *Military Psychology, 23*(6), 616-638. doi: 10.1080/08995605.2011.616792

Espinosa, J. Alberto, Lerch, F. Javier, & Kraut, Robert E. (2009). Explicit Versus Implicit Coordination Mechanisms and Task Dependencies: One Size Does Not Fit All *TEAM COGNITION Understanding the Factors that Drive Process and Performance* (pp. 107-129). Washington DC: American Psychological Association. (Reprinted from: 2009).

Espinosa, J. Alberto, Slaughter, Sandra A., Kraut, Robert E., & Herbsleb, James D. (2007). Team Knowledge and Coordination in Geographically Distributed Software Development. *Journal of Management Information Systems, 24*(1), 135-169.

Fiore, Stephen M., Salas, Eduardo, Cuevas, Haydee M., & Bowers, Clint A. (2003). Distributed coordination space: Toward a theory of distributed team process and performance. *Theoretical Issues in Ergonomics Science, 4*(3-4), 340-364. doi: 10.1080/1463922021000049971

Guillot, Tara L. (2002). Team Building in a Virtual Environment. In S. Sussan (Ed.), *Infoline* (Vol. Issue 0205). United States of America: ASTD Workplace Learning & Performance Press.

Gupta, Manish, Banerjee, Shamik, Agrawal, Manish, & Rao, H. Raghav. (2008). Security analysis of Internet technology components enabling globally distributed workplaces—a framework. *ACM Transactions on Internet Technology, 8*(4), 1-38. doi: 10.1145/1391949.1391951

Mezgár, István. (2003). Role of trust in networked production systems. *Annual Reviews in Control, 27*(2), 247-254. doi: 10.1016/j.arcontrol.2003.09.007

Resick, Christian J., Dickson, Marcus W., Mitchelson, Jacqueline K., Allison, Leslie K., & Clark, Malissa A. (2010). Team composition, cognition, and effectiveness: Examining mental model similarity and accuracy. *Group Dynamics: Theory, Research, and Practice, 14*(2), 174-191. doi: 10.1037/a0018444

Staggers, J., Garcia, S., & Nagelhout, E. (2008). Teamwork Through Team Building: Face-to-Face to Online. *Business Communication Quarterly, 71*(4), 472-487. doi: 10.1177/1080569908325862

Sugar, Steve, & Takacs, George. (2000). *Games that teach teams : 21 activities to super-charge your group!* San Francisco: Jossey-Bass/Pfeiffer.

Thiagarajan, Sivasailam, & Parker, Glenn M. (1999). *Teamwork and teamplay : games and activities for building and training teams*. San Francisco, Calif: Jossey-Bass/Pfeiffer.

6. Appendices

Team 1			
	July	September	Difference
Schedule	2	2	0
stay on task	1	2	1
Networking	1	3	2
Plan/participate meetings	2	3	1
Recognizing feedback	2	3	1
Interaction	2	2	0
Relationship to team	2	2	0
Collaborate	2	2	0
Individual behaviors	3	2	-1
Results	2	2	0
Storage	3	3	0
Technology	3	3	0
Productivity	2	1	-1
Performance measurement	1	2	1
Communicates clearly	2	2	0
Keeps commitments	2	2	0

Team 2			
	July	September	Difference
Schedule	1	2	1
stay on task	2	2	0
Networking	2	2	0
Plan/participate meetings	3	3	0
Recognizing feedback	1	3	2
Interaction	2	3	1
Relationship to team	1	2	1
Collaborate	2	3	1
Individual behaviors	2	2	0
Results	2	3	1
Storage	2	2	0
Technology	2	3	1
Productivity	1	2	1
Performance measurement	1	2	1
Communicates clearly	2	3	1
Keeps commitments	2	2.5	0.5

Team 3

	July	September	Difference
Schedule	2	2	0
stay on task	1	1	0
Networking	2	2	0
Plan/participate meetings	1	2	1
Recognizing feedback	1	2	1
Interaction	3	1	-2
Relationship to team	2	1	-1
Collaborate	2	2	0
Individual behaviors	1	1	0
Results	2	1	-1
Storage	1	1	0
Technology	2	2	0
Productivity	2	2	0
Performance measurement	2	1	-1
Communicates clearly	1	1	0
Keeps commitments	2	1	-1

Team 4

	July	September	Difference
Schedule	2	2	0
stay on task	2	3	1
Networking	1	2	1
Plan/participate meetings	3	3	0
Recognizing feedback	2	2	0
Interaction	1	2	1
Relationship to team	2	2	0
Collaborate	1	2	1
Individual behaviors	2	3	1
Results	1	3	2
Storage	1	3	2
Technology	3	3	0
Productivity	2	2	0
Performance measurement	1	2	1
Communicates clearly	3	2	-1
Keeps commitments	3	3	0

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced