Interested in learning more about security?

SANS Institute InfoSec Reading Room

Bill Gates and Trustworthy Computing: A Case Study in Transformational Leadership

The notion that IT security is a serious issue is non-controversial. The market for cybersecurity spending topped $75 billion in 2015, and analysts expect it to exceed $170 billion by 2020 (Morgan 2016). With the advent of cloud computing, the explosion of mobile devices, and the emergence of increasingly sophisticated adversaries from organized crime and nation-state actors, businesses and the industry as a whole will require the vision of great leaders to keep pace with the threats. We can look to the industry's rich...

Bill Gates and Trustworthy Computing: A Case Study in Transformational Leadership

Author: Preston S. Ackerman, psackerman@gmail.com
Advisors: Dr. Toby Gouker, Stephen Northcutt
Accepted: September 13, 2016

Template Version September 2014

Abstract

The notion that IT security is a serious issue is non-controversial. The market for cybersecurity spending topped $75 billion in 2015, and analysts expect it to exceed $170 billion by 2020 (Morgan 2016). With the advent of cloud computing, the explosion of mobile devices, and the emergence of increasingly sophisticated adversaries from organized crime and nation-state actors, businesses and the industry as a whole will require the vision of great leaders to keep pace with the threats. We can look to the industry's rich history to see examples of such transformational leadership in the past. An enlightening case study is the Microsoft Trustworthy Computing initiative, launched by an insightful and stimulating memo Bill Gates sent on January 15, 2002. The initiative would not only transform culture, procedures, and policy surrounding security at Microsoft, but would in fact cause a dramatic shift for the entire industry. The idealized influence in the leadership shown by Gates can serve as a model for today's leaders.

Introduction

The security challenges facing the information technology industry are myriad. As systems become increasingly complex, software tends to become more vulnerable (Wahsheh, Jr. et al. 2012). This problem is exacerbated by the fact that software developers have traditionally designed software with a focus on functionality, with security often "bolted on" as an afterthought, if at all. After all, security is a non-functional requirement, and not one for which customers typically express a strong desire (Geer 2010). Impactful transformational leadership is necessary for individual businesses and the IT industry as a whole to address future challenges. The four components of transformational leadership are idealized influence, inspirational motivation, individualized consideration, and intellectual stimulation. Although all four can potentially have impact with security issues, one has already proven quite effective in this arena: idealized influence. Idealized influence is defined as "managers who are exemplary role models for associates", who "can be trusted and respected by associates to make good decisions for the organization" (Hall et al. 2015). The power of idealized influence to improve IT security practices is evident through a case study involving Bill Gates and the Trustworthy Computing (TwC) initiative he launched at Microsoft with a January 2002 all-employee memo.

1. Trustworthy Computing - Background

1.1. Microsoft's Security Issues

During the latter part of 2001, Microsoft products suffered a series of significant attacks, frustrating users and according to some experts, even threatening the stability of the internet (Schwartz 2012). A worm called "Code Red" exploited a vulnerability in Microsoft's Internet Information Server (IIS), infecting 300,000 hosts (ibid) and causing an estimated $2 billion in mitigation and productivity costs (Xiao, Witcschey, Murphy-Hill 2014). A variant called "Code Red II" appeared less than a month later (Schwartz 2012). Then, approximately a week after the September 11 terror attacks, a worm called "Nimda" exploited yet another IIS vulnerability (ibid). These devastating and headline-

grabbing attacks on Microsoft's server products, when coupled with the numerous viruses such as "Melissa" and "ILOVEYOU" which users had experienced firsthand through Microsoft's office productivity applications Word and Outlook, left Microsoft's reputation at its nadir (ibid). Indeed, a Gartner report had warned customers to "Run, don't walk, away from IIS" (Bradley 2014).

1.2. The "Trustworthy Computing" Memo

In the aftermath of these significant failures, on January 15, 2002, Bill Gates sent a memo to all Microsoft employees which would result in an immediate change in culture and procedures surrounding secure development at Microsoft, and in fact, would have ripple effects felt throughout the industry (Bradley 2014). Gates declared Microsoft must "lead the industry to a whole new level of Trustworthiness in computing", and went on to define TwC as "computing that is as available, reliable, and secure as electricity, water services and telephony" (Gates 2002). He acknowledged current systems fell well short of that lofty standard, and that the problem went beyond Microsoft. He noted it challenged "the entire computing ecosystem, from individual chips all the way to global Internet services", and would require industry-wide cooperation (ibid). By laying out with great honesty and clarity the problems Microsoft faced, what was at stake if they failed, and a visionary path forward to improve, Bill Gates demonstrated transformational leadership through idealized influence.

1.3. Secure Development Lifecycles

In the TwC Memo, Gates stated that Microsoft needed to implement design approaches which would reduce dramatically the number of security vulnerabilities present in software produced by Microsoft, its partners, and its customers (Gates 2002). From this edict, Microsoft subsequently developed the Secure Development Lifecycle (SDL), a software development methodology adapted from the widely accepted waterfall lifecycle (Shackleford 2011). The guiding principles used to create the methodology were "Secure by Design; Secure by Default; Secure in Deployment; and Communications" (Maurya 2010). Upon its release in 2004, Microsoft mandated implementation of SDL for all products with meaningful risk to the sensitive data of businesses or individuals (ibid).

2. Impact at Microsoft

The security improvements Microsoft products released after TwC and the SDL mandate were significant and immediate. After the Gates memo, Microsoft tasked a small team of employees with deciding how to proceed. They reached the stunning decision to halt development of Windows Server 2003, and redirected focus for the product exclusively on security (Bradley 2014). Indeed, they mandated implementation of SDL[1] and provided security training for everybody assigned to the project (ibid). Microsoft measured SDL's effectiveness through the number of vulnerabilities reported within one year of launch (Lipner and Howard 2005). The first desktop Operating System (OS) developed using SDL was Windows Vista, which had 45% fewer vulnerabilities a year after launch than its predecessor Windows XP (Ashford 2012). SQL Server 2005 resulted in a staggering 91% fewer vulnerabilities than its pre-SDL predecessor SQL Server 2000 (ibid). In the same vein, Windows Server 2003 had a 61% decline in first-year vulnerabilities when compared with Windows Server 2000.

The TwC initiative (including SDL) was successful at Microsoft because, using transformational leadership exhibited through idealized influence, Gates addressed the potential barriers to the effectiveness of such an initiative from the very beginning. Most critically, he demonstrated strong executive support for the effort; he spurred on a change in company culture regarding security; and he ensured employees were trained effectively in the new policies and procedures.

A change as dramatic as the TwC initiative in a company of Microsoft's size required strong executive support. Diffusion of innovation (DOI) theory has shown "highly influential early adopters and organizational mandates can increase both the probability and speed of adoption" (Xiao, Witschey, Murphy-Hill 2014). The Gates memo demonstrated full buy-in to the concept of TwC from the most influential of all early adopters at the company, and the formalized requirement to apply SDL across a broad range of Microsoft products came soon after (Lipner and Howard 2005).

[1] Although SDL was still a work in progress, most of its processes were implemented in the development of Windows Server 2003.

Author Name, email@address

Company culture is another key factor in the adoption of security tools and practices (Xiao, Witschey, Murphy-Hill 2014). In his memo, Gates made a powerful statement for change in Microsoft's security culture:

> "So now, when we face a choice between adding features, and resolving security issues, we need to choose security. …If we discover a risk that a feature could compromise someone's privacy, that problem gets solved first."

He also called for active involvement of all employees when he wrote, "I encourage everyone at Microsoft to look at what we've done so far and think about how they can contribute."

Availability of training is another factor which can contribute toward adoption of security tools (Xiao, Witschey, Murphy-Hill 2014). When Microsoft redirected Windows Server 2003 development efforts midstream, it sent almost 10,000 developers to bootcamp-type training (Bradley 2014). Microsoft also understood the changing threat landscape and thus required annual updates to the training (Lipner and Howard 2005).

The emphasis on security was outwardly noticeable in Microsoft's products. Windows Vista was viewed by many as a failure, but the OS introduced key security features which strengthened the platform's security and have remained a factor in subsequent versions, such as preventing kernel overwrites by malware through Patchguard; reduction in buffer overruns through address space randomization; secure data encryption through Bitlocker; anti-malware functionality through Windows Defender; and prompting users for tasks requiring administrative privileges (which many types of malware require) through User Account Control (Schwartz 2012). Gates had the vision to focus on the long-term stability of Microsoft's products as opposed to worrying about quarterly profits by focusing on less important functionality. The impact of TwC at Microsoft was undeniable, and the metrics demonstrate its effectiveness.

3. Impact Industry-wide

The language Bill Gates used in the TwC memo showed he clearly understood the initiative to be larger than Microsoft from the outset. In many parts of the memo, his

language went beyond being specific to Microsoft and was instead inclusive of the whole industry, as seen in the following phrases (emphasis added):

"We must *lead the industry* to a whole new level..."
"We're driving... standards so that *systems from all vendors*..."
"Microsoft *and the computer industry* will only succeed in that world if..."
"The challenge here is one that *Microsoft is uniquely suited to solve*." (Gates 2002)

Following the bold transformational leadership exhibited by Gates, Microsoft indeed proceeded to be an industry thought leader regarding matters of security. Microsoft's SDL was the first process for secure development, and Microsoft's SDL-Agile subsequently adapted the process for an agile lifecycle (Geer 2010). Microsoft chose to make the SDL process and the tools created to implement it freely available, along with Microsoft Press books about secure design, coding, and threat modeling (Lipner and Howard 2005; Ashford 2012).

The release of Microsoft's SDL methodology sparked a trend. Other organizations have since released comparable processes, to include OWASP's Comprehensive, Lightweight Application Security Process (CLASP); the Building Security in Maturity Model (BSIMM); the Secure Software Development Lifecycle (SSDL); the Software Assurance Maturity Model (SAMM) (Geer 2010); and the Rugged Software Manifesto (Shackleford 2011). Other major companies such as Cisco and Adobe have built internal secure development practices around Microsoft's SDL (Ashford 2012).

Adoption of SDLs within the industry has not been unanimous, but it is has been substantial and continued to trend upward. A 2010 survey of software developers revealed 81% of respondents were familiar with formal secure coding methodologies, but only 30.4% stated they were using them (Geer 2010). SDLs have been accepted more readily in large enterprises (Geer 2013). Compliance standards such as Payment Card Industry (PCI) have served as a driver for increased adoption, but some companies have instead chosen to become compliant by merely protecting bad code through the use of a Web Application Firewall (ibid). The vertical market which has shown the most headway in secure development is finance. BITS, a group of 100 of the largest financial service

providers, has incorporated many of the features of Microsoft's SDL in their Software Assurance Framework (ibid).

As part of the TwC initiative, Microsoft participated in a variety of efforts to fight cybercrime and improve security in ways other than secure development. For example, they formed an innovative cooperative effort with legal and technical teams to combat cybercrime called the Microsoft Digital Crimes Unit, or DCU (Ashford 2012). The DCU cooperated with law enforcement to take down the command and control structure of botnets such as Zeus (Schwartz 2012). In 2011, Microsoft created the Blue Hat Prize, a contest which challenges security professionals to innovate cyber defense approaches (Ashford 2012). Microsoft also formed a security council composed of top IT security professionals which meets bi-annually in Redmond (Schwartz 2012).

Another indicator of TwC's success is its longevity. Gates authored the memo in 2002, yet in 2012 a number of ten-year retrospectives were published about its current state. Microsoft refreshed the initiative with “TwC Next”, which provides updated perspectives related to changes in the landscape such as cloud storage and big data (Charney 2012). Outside parties have also continued to pursue updates to the TwC concept for the era of mobile and cloud technologies (Banga, Crosby, and Pratt 2014).

The industry-wide impact of TwC is clear based on the similar security models which followed after SDL; the significant adoption of secure coding methodologies; the industry initiatives Microsoft has participated in such as the DCU and the Blue Hat Prize; and the extension of the model to next-generation technologies by Microsoft and others.

4. Conclusion

Nobody would suggest Microsoft's TwC initiative solved all security problems facing the IT industry – one need look no further than the headlines of any given day to know otherwise. It would also be unreasonable, however, to conclude that Gates' TwC memo did not have a substantial positive impact on the industry's ability to cope with its ongoing security issues. It took the idealized influence of an exemplary transformational leader to have such an impact, achieving many of the hallmarks of transformational leadership such as vision, empowering others, leading by example, working

cooperatively with others, and acting as an agent of change (Hall et al. 2015). This case study provides an example which can benefit leaders of today and in the future.

Author Name, email@address

References

Ashford, W. (2012, January). Microsoft: Is computing more trustworthy 10 years on? Retrieved August 21, 2016, from http://www.computerweekly.com/feature/Microsoft-Is-computing-more-trustworthy-10-years-on

Banga, G., Crosby, S., & Pratt, I. (2014). Trustworthy Computing for the Cloud-Mobile Era: A Leap Forward in Systems Architecture. IEEE Consumer Electron. Mag. IEEE Consumer Electronics Magazine, 3(4), 31-39. doi:10.1109/mce.2014.2338591

Bradley, T. (2014, March 5). The Business World Owes a Lot to Microsoft Trustworthy Computing. Retrieved August 21, 2016, from http://www.forbes.com/sites/tonybradley/2014/03/05/the-business-world-owes-a-lot-to-microsoft-trustworthy-computing/

Charney, S. (2012, February 28). Trustworthy Computing Next. Retrieved August 24, 2016, from http://aka.ms/twcnextwp

Gates, B. (2002, January 15). Trustworthy Computing Memo [Letter to Microsoft].

Geer, D. (2010). Are Companies Actually Using Secure Development Life Cycles? Computer, 43(6), 12-16. doi:10.1109/mc.2010.159

Geer, D. (2013, April 29). Secure Development Lifecycles Eding Further Into the Market [Web log post]. Retrieved August 21, 2016, from http://blog.smartbear.com/codereviewer/secure-development-lifecycles-edging-further-into-the-market/

Hall, J., Johnson, S., Wysocki, A., Kepner, K., Farnsworth, D., & Clark, J. L. (2015, October). Transformational Leadership: The Transformation of ... Retrieved August 21, 2016, from http://edis.ifas.ufl.edu/pdffiles/HR/HR02000.pdf

Jr., C. S., Wahsheh, L. A., Ahmad, A., Graham, J. M., Hinds, C. V., Williams, A. T., & Deloatch, S. J. (2012). Software Security: The Dangerous Afterthought. 2012 Ninth International Conference on Information Technology - New Generations. doi:10.1109/itng.2012.60

Author Name, email@address

Lipner, S. (n.d.). The Trustworthy Computing Security Development Lifecycle. 20th Annual Computer Security Applications Conference. doi:10.1109/csac.2004.41

Maurya, H. (2010, January 14). Microsoft Security Development Lifecycle ... - TechSurface. Retrieved August 25, 2016, from http://techsurface.com/2010/01/microsoft-security-development-lifecycle-sdl.html

Morgan, S. (2016, March 9). "Worldwide Cybersecurity Spending Increasing To $170 Billion By 2020" Retrieved August 30, 2016, from http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/

Shackleford, D. (2011, September). Integrating Security into Development, No Pain - SANS ... Retrieved August 21, 2016, from https://www.sans.org/reading-room/whitepapers/analyst/integrating-security-development-pain-required-35060

Schwartz, J. (2012, May 10). 10 Years of Trustworthy Computing: The Current State of Windows Security -- Redmondmag.com. Retrieved August 24, 2016, from https://redmondmag.com/articles/2012/05/01/10-years-of-trust.aspx

Xiao, S., Witschey, J., & Murphy-Hill, E. (2014). Social influences on secure development tool adoption. Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '14. doi:10.1145/2531602.2531722

Author Name, email@address

Last Updated: June 27th, 2017

Upcoming SANS Training

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

SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SEC564:Red Team Ops	OnlineCAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced