Journal of Cyber Policy

Firmware-Based Threats

February, 2018

Contact
Hugh Taylor
Executive Editor
Journal of Cyber Policy
www.journalofcyberpolicy.com
info@journalofcyberpolicy.com
(310) 383-7041

Abstract
Firmware is a cyberattack vector. While public attention focuses on cyberattacks and data breaches conducted over networks with software-borne malware, the risk of malicious code embedded in the firmware of millions of digital devices poses a potentially more serious threat to cybersecurity. This report reviews how security professionals view the firmware threat as well as their impression of the tech industry's readiness to detect and prevent a firmware-based attack.

Executive Summary

Malicious code embedded in the firmware of millions of digital devices poses a serious threat to cybersecurity. The risk is due to several factors, including the stealthy nature of firmware-borne threats and the possibility that adversarial nations, such as China, are embedding malware in firmware at the manufacturing stage.

This report reviews how security professionals view the firmware threat as well as their impression about the tech industry's readiness to detect and prevent a firmware-based attack. It is based on a survey and some interviews done with thought leaders. The highlights include:

- 57% of survey respondents felt that firmware threats were a "serious security threat" or "the most serious security threat possible."
- 37% thought firmware represented a threat that needed to be addressed. None thought firmware didn't pose a threat.
- 64% felt that a firmware-based threat could have a serious or catastrphic impact, though the threat is partially mitigated by the difficulty of creating malware on firmware.
- 64% identified Internet of Things (IoT) devices as the most vulnerable to firmware-borne threats.
- 78% did not think the tech industry is doing enough to defend consumers, business and government device users from firmware-based malware.
- 36% percent felt their orgnaizations were prepared for a firmware-based attack. 35% were either not prepared or didn't know.

Table of Contents

Introduction

While the media and IT industry focus on cyberattacks and data breaches conducted over networks with software-borne malware, another, perhaps more dangerous threat remains relatively obscure. Malicious code embedded in the firmware of millions of digital devices poses a serious threat to cybersecurity. The following report reviews how security professionals perceive the firmware threat as well as their impression of the tech industry's readiness to detect and prevent a firmware-based attack.

The Survey and Interviews

This report is based on survey and interviews. The sample size is small, so it should not be seen as statistically significant. However, even with small numbers, several points of consensus appear to be evident. The interviews offer additional insight into how experienced cybersecurity professionals see the firmware threat. The respondents are all from North America and work in a range of industries in organizations of between 100 and over 5,000 employees. The Appendix contains survey details.

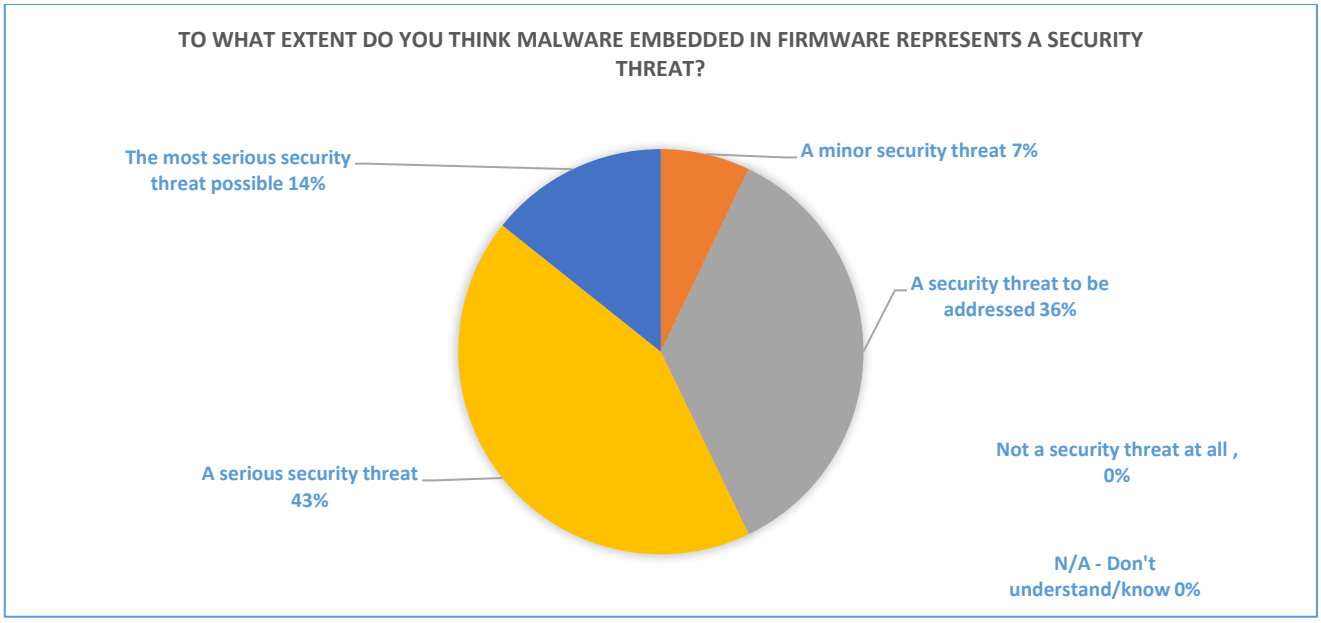
The Firmware Threat

Virtually all digital devices, from smart phones to servers, disk arrays and network appliances, contain firmware. Firmware is software that is written onto the circuitry itself. Firmware is what enables the device to work so the operating system and application software can function. The Basic Input/Output System (BIOS) software on a PC chip is an example of firmware.

Firmware is typically installed by the device manufacturer, though the firmware code itself might be written by the manufacturer's customer. For example, a company that designs smart phones might create firmware code for its device. It will send that code to a contracted manufacturer for installation on the device's silicon chips.

The firmware risk comes from the potential to corrupt the firmware code. This can happen at the manufacturing stage or at some point in time after. Firmware can be infected with malware. Firmware-borne malware can hijack root access to a device, steal data or even simply turn the device off, permanently. This is known as "bricking" a device. Unable to switch on, it effectively becomes a "brick." The attack on Saudi Aramco (suspected to be an Iranian retaliation for the Stuxnet virus) caused the bricking of 30,000 computers through a firmware attack.

Firmware can be infected with malware. Firmware-borne malware can hijack root access to a device, steal data or even simply turn the device off. Permanently. This is known as "bricking" a device.



Fifty-seven percent of survey respondents felt that firmware threats were “serious security threat” or “the most serious security threat possible.” Thirty-seven percent thought firmware represented a threat that needed to be addressed. None thought firmware didn’t pose a threat. A survey respondent commented, “As we've seen with Equation Group implants in hard drive firmware, this is a serious threat, with potentially catastrophic impact given the proper placement.”

According to Kris Lovejoy, former CSO of IBM and now CEO of BluVector, whose technology uses AI to detect threats on networks, “All embedded devices are at risk.” Lovejoy explained that there are three layers in a digital device. There is the chip, the device manufacturer and the device “maker,” which is usually just adding an interface, application software and a brand name to a piece of equipment almost wholly made by others.

Lovejoy noted, “The problem with this process is there is no entity in any part of that supply chain that has any incentive, any expertise, any ability to patch or manage the whole. These devices have been built and deployed by people who want to keep their margins as high as possible. It's not in their financial interest to layer on a lot of security capabilities, and maintaining these older things is not a priority, especially when these devices are selling for pennies or a couple of bucks a piece. It’s a perfect storm -- very old components, some of which are customized, some open source, and most really old. They can't be upgraded, they can't be patched.”

“There is no entity in any part of that supply chain that has any incentive, any expertise, any ability to patch or manage the whole.”

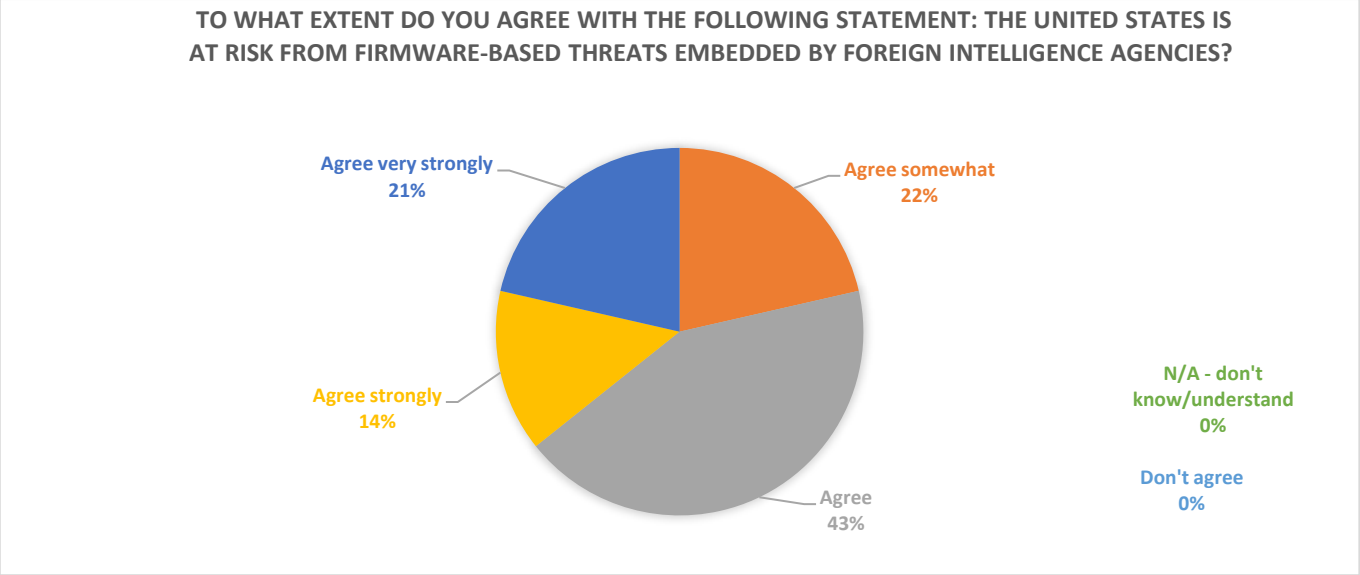
Kris Lovejoy

CEO of BluVector

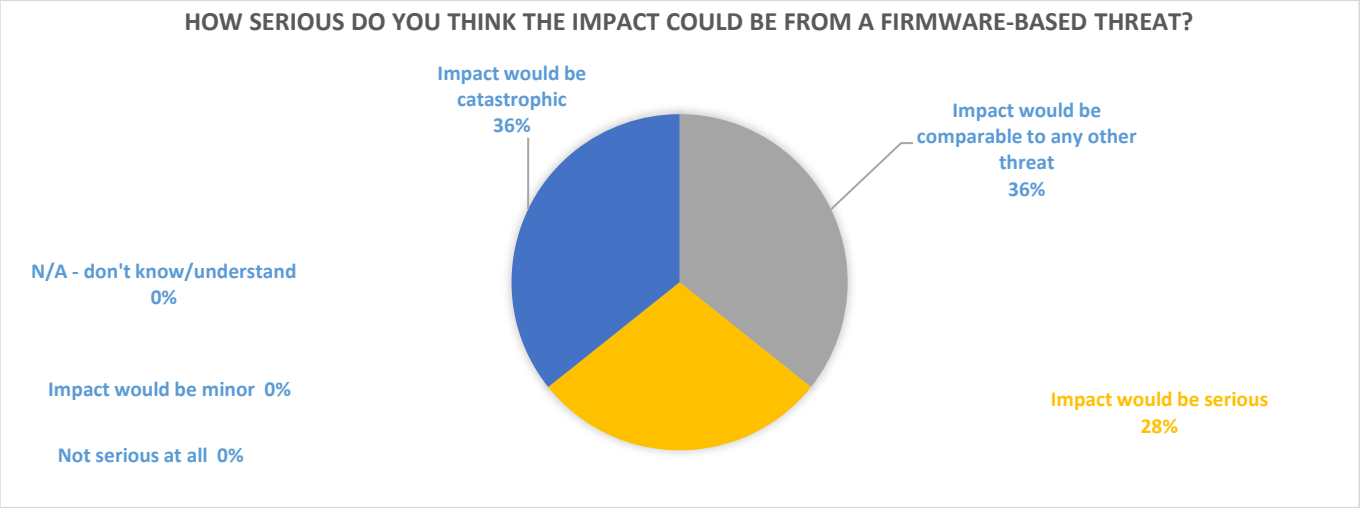
and Former CSO of IBM

Why is the Firmware Threat Potentially Serious?

One of the main reasons firmware-borne threats present a serious risk is because they represent a potent, stealthy vector of attack from the United States’ strategic adversaries. The vast majority of electronic components originate in China, a global rival to the United States. China is also the main hub of electronics manufacturing. Given China’s complicated relationship with the United States, it is not unreasonable to suspect that that country’s intelligence services are embedding malware into devices shipped to the United States. The majority of survey respondents agree that the United States is at risk from firmware-based threats embedded by foreign intelligence services.



Jason McNew, a former Air Force officer and White House cybersecurity staffer with the highest level of security clearance, is afraid of malware contained in Chinese-made electronics. He spoke on the issue by saying, “China is authoritarian and they [the government] direct a lot of the economy. There's not a lot of room between these different [intelligence] entities and some of the manufacturers that are over there. I can't get into specifics, but it's already been disclosed that when we buy integrated circuits, applications, specific integrated circuits that come from that region, that we've got caught back doors in them.”



Survey respondents expressed a comparable fear. Nearly two thirds felt that a firmware-based threat could have a serious or catastrophic impact. One mitigating factor is the difficulty of creating such a threat, as a one respondent commented. “Firmware-based malware is highly advanced, and difficult to do well. But, the industry needs to anticipate its ubiquity.” In terms of ubiquity, 64% of survey respondents identified Internet of Things (IoT) devices as the most vulnerable to firmware-borne threats.

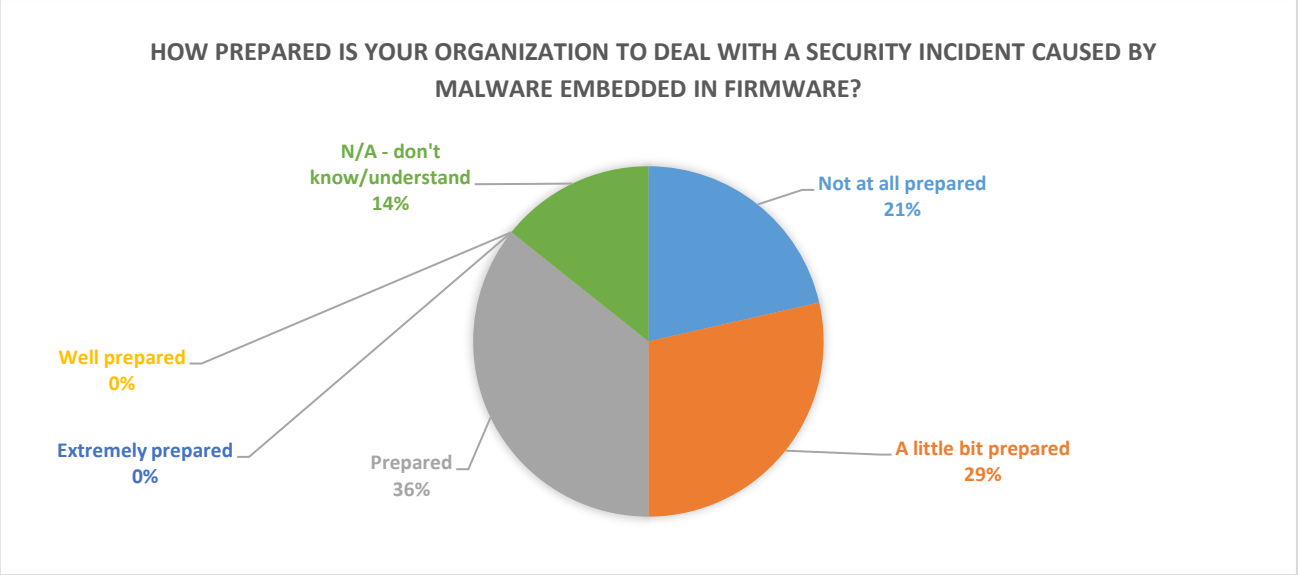
Firmware is a serious threat not only because of its ubiquity and origin in adversarial regions. It is also extremely hard to detect. As a survey respondent noted, “Firmware based threats are the most difficult to detect and to remove.” Steven Sprague, CEO of Wave Systems and a longtime participant in Trusted computing initiatives, explained, “It's one of the really open and interesting science problems that's out there right now, determining that somebody hasn't tinkered with that [silicon] product in some way, shape or form and introduced a weakness. And those weaknesses can be exploited and they can be exploited globally. It hasn't really happened yet at scale in a way that has really done a lot of damage.”

Stewart Kantor, CEO of Full Spectrum, which builds secure networks for critical infrastructure, concurred. He said malware in firmware "could be written in it at the beginning. There are all sorts of vulnerabilities where a device boots and launches malicious code. There's been a number of occasions where issues like that have occurred."

To understand the problem better, listen to Robert Wood, a security consultant, describe how hackers can hide code in firmware. "When Android netware code is packaged up, one of the things that both legitimate and illegitimate developers, like malware developers, can do is put it through this process called obfuscation. That is basically where you're taking a piece of the package, whether it's a proprietary algorithm or potentially something malicious that you want to hide, and you can make it harder to analyze. You can encrypt the class names, you can scramble things, you can mislabel things. There's a whole bunch of obfuscation techniques. And it makes the analysis of that code much harder."

How Prepared is the Tech Industry for a Firmware-Borne Cyberattack?

Seventy-eight percent of survey respondents did not think the tech industry is doing enough to defend consumers, business and government device users from firmware-based malware? In terms of their own organizations, however, the numbers are a bit more promising. Thirty-six percent felt their orgnaizations were prepared for a firmware-based attack. Still, 35% were either not prepared or didn't know. The takeaway is that more could certainly be done to get the United States ready to deal with firmware-based threats.



Conclusion

The survey and interviews clearly show that firmware-based threats are real and quite serious. Due to stealth and the risk of malware being embedded by adversarial nations, the issue deserves attention. The IT industry is not perceived as doing enough to defend against the threat. At the same time, effective firmware-based malware is difficult to create, so the risk is somewhat self-limiting.

What can be done about the problem? The survey and interviews suggest that a better job needs to be done with the digital device supply chain. As one respondent said, "I think there needs to be better testing before these consumer, business and government devices are put to market. Often times, they are rushed and vulnerabilities are overlooked." Such practices would surely help. In the meantime, it is up to individual organizations to take responsibility for potential risks in the firmware of their hardware infrastructures and digital devices.

Appendix – Survey Questions and Responses

1. What industry do you work in?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
EDUCATION AND HEALTH SERVICES	4		29
FINANCIAL ACTIVITIES	2		14
GOVERNMENT	2		14
INFORMATION	2		14
OTHER SERVICES (EXCEPT PUBLIC ADMINISTRATION)	1		7
PROFESSIONAL AND BUSINESS SERVICES	1		7
Other	2	1. Information Security 2. Media and Telecommunications	14
	Total respondents: 14 **Skipped question: 0**	0% 20% 40% 60% 80%	

2. What region are you in?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
North America	14		100
Latin America	0		0
EMEA	0		0
Asia	0		0
Other	0		0
	Total respondents: 14 **Skipped question: 0**	0% 20% 40% 60% 80%	

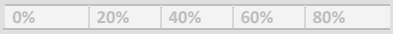
3. What size organization do you work for?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
1-100 employees	5		36
101-1000 employees	3		21
1001-5000 employees	1		7
Over 5,000 employees	5		36
	Total respondents: 14 **Skipped question: 0**	0% 20% 40% 60% 80%	

4. What is your primary job role?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
Corporate/organizational management	4		29
Information technology	1		7
Information security	6		43
Support staff	0		0
Other	3		21

Total respondents: 14
Skipped question: 0

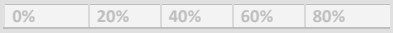


5. To what extent do you think malware embedded in firmware represents a security threat?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
1 Not a security threat at all	0		0
2 A minor security threat	1		7
3 A security threat to be addressed	5		36
4 A serious security threat	6		43
5 The most serious security threat possible	2		14
- N/A - Don't understand/know	0		0

Average: 3.64 — Median: 4

Total respondents: 14
Skipped question: 0

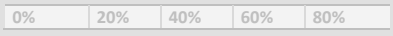


6. How serious do you think the impact could be from a firmware-based threat?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
1 Not serious at all	0		0
2 Impact would be minor	0		0
3 Impact would be comparable to any other threat	5		36
4 Impact would be serious	4		29
5 Impact would be catastrophic	5		36
- N/A - don't know/understand	0		0

Average: 4 — Median: 4

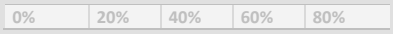
Total respondents: 14
Skipped question: 0



7. What kinds of devices do you think are most vulnerable to firmware-based malware?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
Mobile devices (smart phones)	0		0
Internet of Things (IoT) devices/sensors	9		64
PCs/Macs	3		21
Tablets	0		0
Home electronics (e.g. Alexa)	0		0
Servers	0		0
Storage arrays	0		0
Network appliances	0		0
Other	2	 "As we've seen with Equation Group implants in hard drive firmware, this is a serious threat, with potentially catastrophic impact given the proper placement."	14

Total respondents: 14
Skipped question: 0

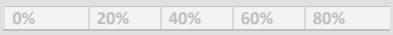


8. To what extent do you agree with the following statement: The United States is at risk from firmware-based threats embedded by foreign intelligence agencies?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
1 Don't agree	0		0
2 Agree somewhat	3		21
3 Agree	6		43
4 Agree strongly	2		14
5 Agree very strongly	3		21
- N/A - don't know/understand	0		0

Average: 3.36 — Median: 3

Total respondents: 14
Skipped question: 0



9. How prepared is your organization to deal with a security incident caused by malware embedded in firmware?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
1 Not at all prepared	3		21
2 A little bit prepared	4		29
3 Prepared	5		36
4 Well prepared	0		0
5 Extremely prepared	0		0
- N/A - don't know/understand	2		14

Average: 2.17 — Median: 2

Total respondents: 14
Skipped question: 0

0% 20% 40% 60% 80%

10. Does your organization have policies designed to mitigate the risk of firmware-based malware?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
Yes	4		29
No	5		36
Other, please specify	5	• Don't know. I do not have much direct contact with university IT policy. • Not specific to firmware but to the symptoms or outcomes with respect to a firmware-based malware . . . . • To some degree through controlling the purchase process of company owned equipment	36

Total respondents: 14
Skipped question: 0

0% 20% 40% 60% 80%

11. Do you think the tech industry is doing enough to defend consumers, business and government device users from firmware-based malware?
(Each respondent could choose only ONE of the following responses.)

Response	Total	% of responses	%
Yes	2		14
No	11		79
Other, please specify	1		7

Total respondents: 14
Skipped question: 0

0% 20% 40% 60% 80%

About Journal of Cyber Policy

Journal of Cyber Policy presents important topics related to cybersecurity policy in plain English. The Journal's goal is to inform while stimulating productive conversations among all security stakeholders.

Hugh Taylor | Executive Editor

Hugh Taylor is a Certified Information Security Manager (CISM) who has written about cybersecurity, compliance and enterprise technology for such clients as Microsoft, IBM, SAP, HPE, Oracle, Google and Advanced Micro Devices. Prior to launching his freelance writing career, he served in executive roles at Microsoft, IBM and several venture-backed technology startups. He has been a lecturer at the University of California, Berkeley's Law School and Graduate School of Information. Hugh is the author of the books B2B Technology Marketing, Event-Driven Architecture: How SOA Enables the Real-Time Enterprise, The Joy of SOX: Why Sarbanes Oxley and Service-Oriented Architecture May Be The Best Thing That Ever Happened To You, and Understanding Enterprise SOA.

Hugh has delivered presentations at industry conferences such as the Institute of Internal Auditors (IIA), the Microsoft Business Process Modeling and SOA conference, the HP Technology Forum and IBM Rational DeveloperWorks. He has consulted with dozens of entrepreneurs and crafted business plans that have helped these new ventures get funded. He earned his AB, Magna Cum Laude from Harvard College in 1988 and his MBA from Harvard Business School in 1992. He lives in Cleveland, Ohio. Prior to working in the technology field, Hugh was a producer of TV movies.

www.journalofcyberpolicy.com