A Forrester Consulting
Thought Leadership Paper
Commissioned By Dell

June 2019

BIOS Security – The Next Frontier for Endpoint Protection

Today’s Threats Upend Traditional Security Measures

Table Of Contents

Project Director:
Sheye Daniels,
Market Impact Associate
Consultant

Contributing Research:
Forrester's Infrastructure &
Operations research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

The BIOS has emerged as a new and unique avenue for attack. If your hardware is breached, the entire operating system falls into jeopardy. Private personal data can become compromised, and computers can lose the ability to communicate with one another, leading to potentially systemic damages throughout an organization.

Executive Summary

Everyone is familiar with the process of booting up a computer. Many of us do this every day — pressing the power button, hearing the startup sound, and seeing the home screen appear. But even some tech professionals may not be aware of what's happening under the surface of their computers. When the CPU of any computer is booted, it communicates with an internal firmware chip called the BIOS (basic input/output system). This BIOS — a tiny hardware microchip hidden within the computer's motherboard — acts as the gate to all the computer's hardware and it gives the commands for how each piece of hardware is supposed to behave and interact. The BIOS is considered one of the most valuable parts of a computing system because of its crucial role to the overall operating system. Without the BIOS firmware chip, your computer wouldn't even be able to load its home screen. Something many of us take for granted.

As security technologies become more sophisticated, cyber criminals find themselves with fewer places to hide and fewer methods to breach computer systems. As a result, attackers are hunting for new infiltration methods. As malicious invaders develop new ways to bypass security systems, organizations must adapt their security strategies to avoid vulnerabilities to hardware-level security breaches.

In March 2019, Dell commissioned Forrester Consulting to evaluate the evolving IT and security needs of companies managing beaches to their hardware- and silicon-level devices and supply chains. Forrester conducted an online survey with 307 IT, security, risk, and compliance decision makers at companies with more than 500 employees to explore this topic. We found that:

KEY FINDINGS

› **Attackers have already begun breaching security at the BIOS level.** Hardware- and silicon-level exploits are a pervasive threat. Nearly two-thirds (63%) of companies have experienced a data compromise or breach within the past 12 months due to an exploited vulnerability in hardware- or silicon-level security.

› **Hardware security initiatives are largely inconsistent and ineffective.** While the majority of organizations reported hardware and endpoint security measures as their top security priorities for the coming year, when asked specifically about hardware-level defenses and supply chain protections, they admitted they weren't properly prepared to address vulnerabilities at these levels. This gap between strategy and execution is exposing firms to potential risk.

› **The complexity of hardware breaches leaves organizations struggling to prevent or address damage.** Attacks to the computer's hardware can come from a seemingly endless number of different ways. Defending against every possible avenue is daunting. Relying on hardware security vendors is key. Organizations are turning to hardware security vendors to help fill gaps, but not all vendors are created equal: just 28% of interviewed organizations are satisfied with their vendors' hardware security management.

Organizations Are Under Increasing Pressure To Respond To Hardware-Level Attacks

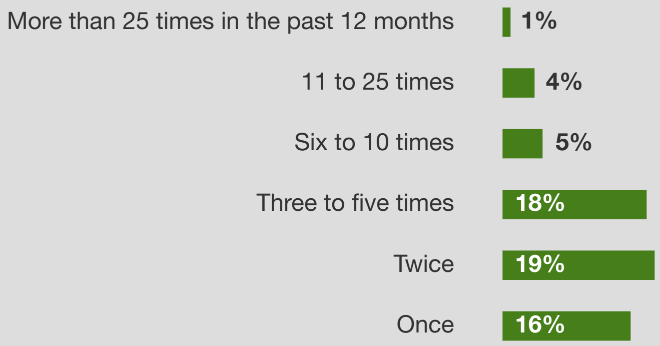
Companies invest significant resources in sophisticated controls to protect people, brand, and assets from cyber criminals. But securing the BIOS and similar hardware attacks comes with its own set of unique challenges to navigate. Properly protecting oneself against multichannel hardware threats takes careful preparation and resources. Despite investments, companies are struggling to optimize their hardware-level security practices. This results in slowed productivity, jeopardized customer loyalty, and compromised employee safety. As hardware-security breaches are becoming harder to prevent, firms are turning toward specialized hardware security vendors to provide a comprehensive and trusted approach to hardware and supply chain security. Even then, not all vendors are created equal. Finding the right hardware-security partner requires a robust strategy from the get-go. Our survey revealed that:

- **Hardware-level systems are a prime target for cyber criminal attacks.** If companies do not proactively prepare for the possibility of hardware threats, then they should brace themselves for attack. The majority of organizations reported experiencing at least one hardware breach in the last 12 months. Of the 307 firms surveyed, 47% experienced at least two hardware-level attacks in the last 12 months (see Figure 1).
- **The types of threats that organizations deal with vary widely, adding complexity to preparation and response plans.** IT and security managers need to protect their supply chains from a swath of hardware-level breaches (see Figure 2). These attacks can be carried out via targeting software vulnerabilities (43%), web application attacks (40%), and strategic web compromises (30%). The intricacy of necessary security procedures makes full-coverage protection even harder to achieve.

Organizations reported experiencing three security breaches on average to the hardware or silicon level within the past year.

Figure 1

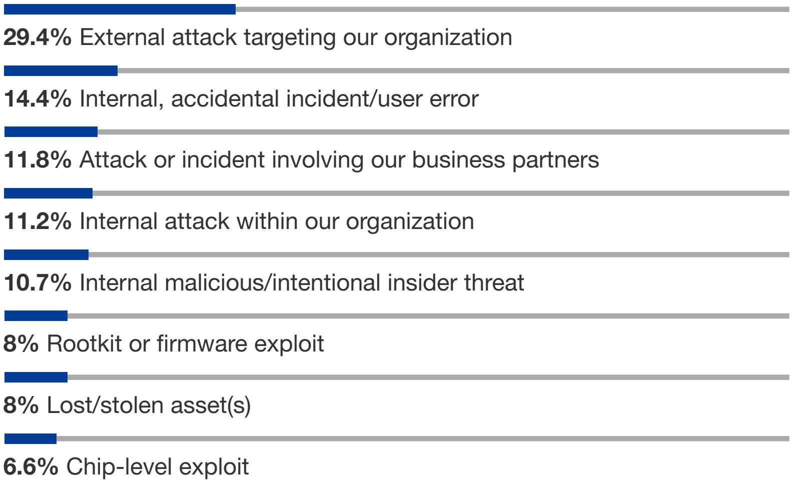
"How many times do you estimate that your firm's sensitive data was potentially compromised or breached in the past 12 months due to a breach in hardware or silicon-level security?"



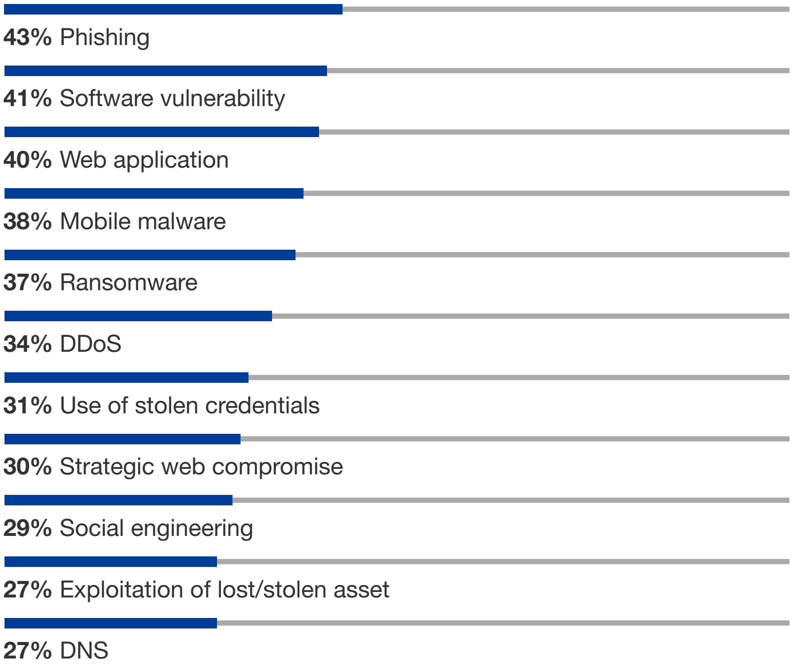
Base: 307 IT, security, or risk and compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

Figure 2

“Of the data breaches experienced in the past 12 months that were attributed to a breach in hardware- or silicon-level security, what percent fall into the following categories?” (Showing mean %)



“How were the external attacks carried out?”



Base: 189 IT, security, or risk and compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

Biggest challenge in securing the hardware supply chain:

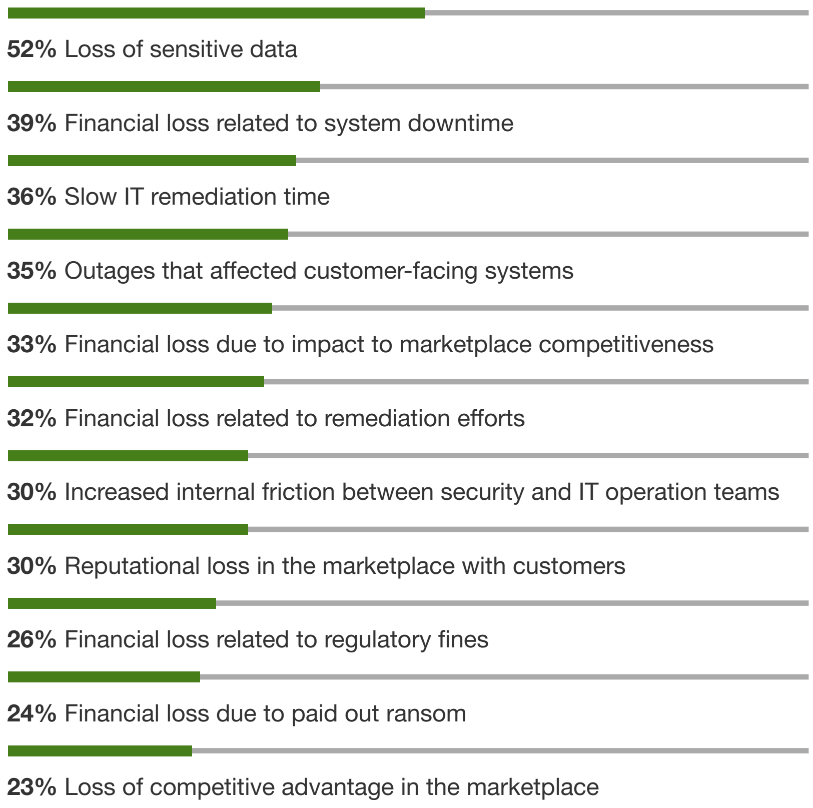
“The ever increasing sophistication of **security threats.”**

IT and security director at a US enterprise

- **These threats put customers and employees in jeopardy, cause brand damage, and impact revenue performance.** Security breaches to the hardware supply chain hinder ongoing operational activity, placing an organization's bottom-line at risk. Companies have a responsibility to shield their employees, customers, partners, and investors from serious reputational and financial harm (see Figure 3).

Figure 3

"Whether or not your organization experienced a hardware or silicon compromise at the device level over the past 12 months, what are the potential, or actual, consequences to the business?"



Base: 307 IT, security, or risk & compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

The complex ripple effects of even one hardware- or silicon-level breach can result in widespread and severe organizational damage.

Current Strategies Don’t Properly Prepare For Hardware-Level Attacks

The companies in our study have already begun looking at ways to optimize BIOS and hardware-level security, and they have started to mature their tools and procedures to better defend from attacks to the hardware supply chain. When we asked firms about their specific IT initiatives, they revealed a maturity disconnect on hardware protection priorities. This is proof that companies have more work to do before they can call themselves secure. Our study showed that:

› **Firms are not as secure as they think they are.** There’s a gap in how much organizations feel they should prioritize and invest into hardware- and silicon-level supply chain security and their actual perception of the risk of those threats, leaving them vulnerable for attack. Despite the fact that nearly two-thirds of organizations recognize they have a moderate to extremely high level of exposure to threats to the hardware supply chain, just 59% have implemented a hardware supply chain security strategy. This discrepancy reveals a lack of consistent preparation, education, or ability to execute on hardware-level security measures (see Figure 4).

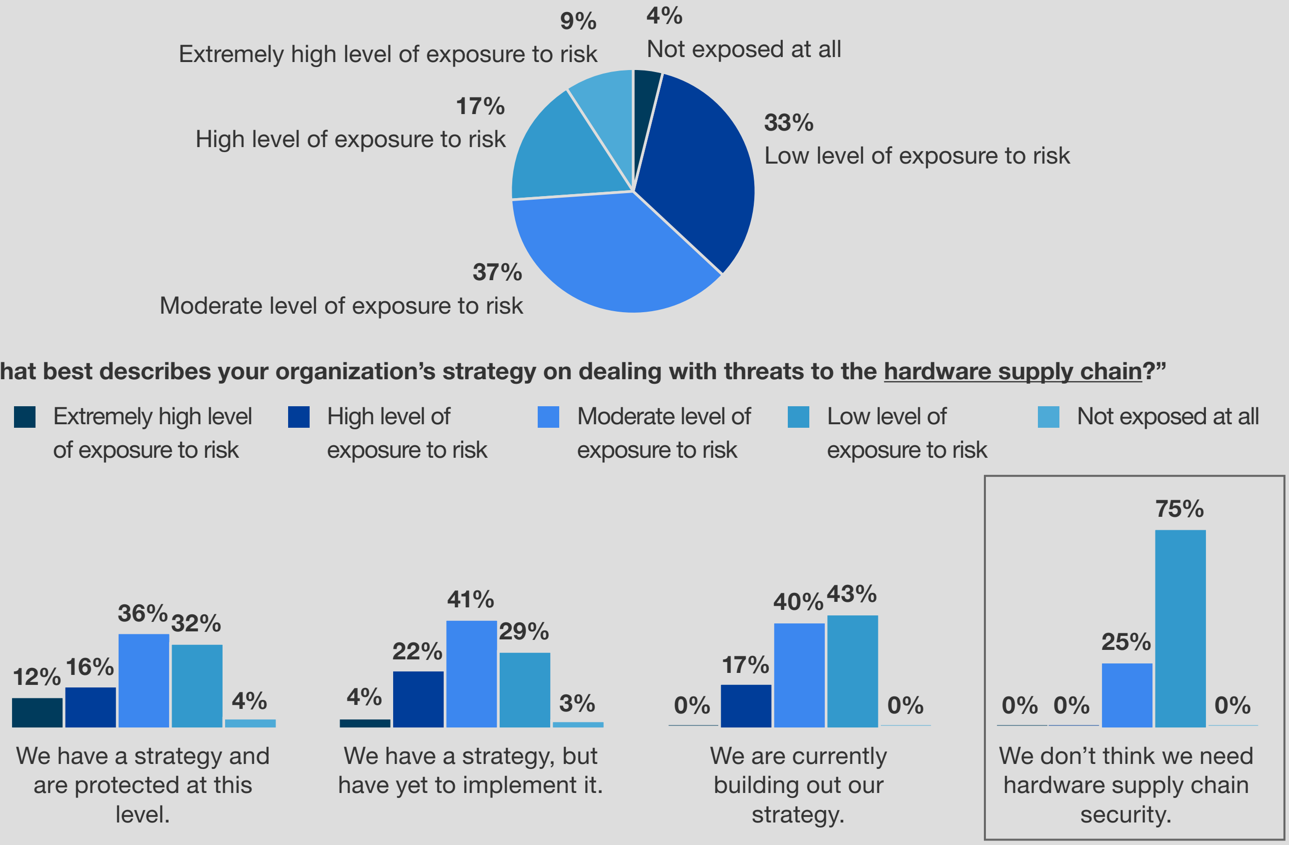
Biggest challenge in securing the hardware supply chain:

“Differing systems, **a lack of integrated approach**, a lack of investment, and differing priorities throughout our supply chain.”

IT and security director at a US enterprise

Figure 4

“What do you feel is your enterprise’s overall level of exposure to threats to the hardware supply chain?”



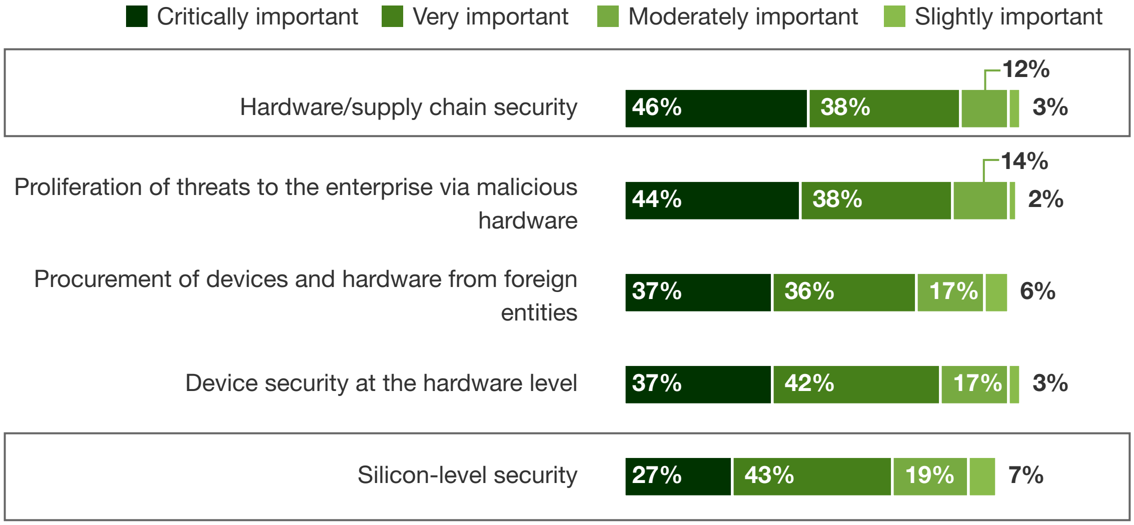
“What best describes your organization’s strategy on dealing with threats to the hardware supply chain?”

Base: 307 IT, security, or risk and compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

- **Current security strategies don’t sufficiently address the spectrum of hardware vulnerabilities.** Seven out of 10 firms identify silicon-level security as very or critically important to overcoming security challenges (see Figure 5). Yet, when asked specifically which security concerns are most prevalent, most firms are inconsistent with their perceptions. Although 60% of firms see BIOS and firmware exploits as being “very” or “extremely” concerning, only half of the surveyed firms feel the same for silicon-level vulnerabilities. This lack of consistency ultimately exposes firms to further risks. If even one channel is left unprotected, a breach can occur.
- **Firms are not properly defending themselves, and thus, struggle against hardware-level security breaches year after year.** The lack of a consistent security approach for defending against hardware-level breaches exposes organizations to the risk of damage, e.g., loss of sensitive data or financial loss. On top of this, it has become more difficult to prevent or remediate the fallout from these breaches over the past year (see Figure 6).

Figure 5

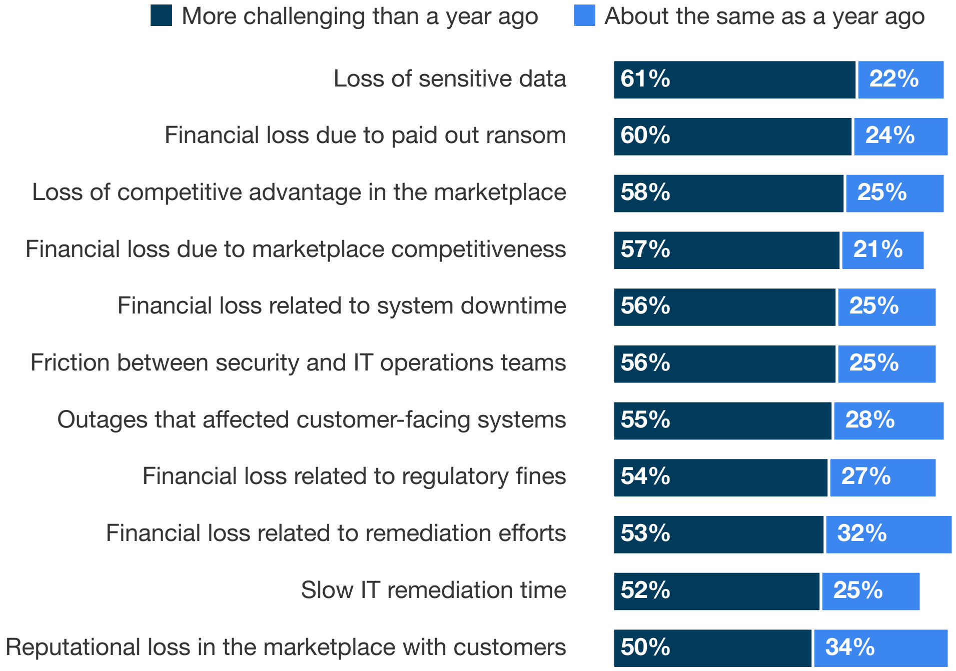
“How important are the following IT security measures/activities in helping your organization overcome the challenges you face in securing your organization?”



Base: 307 IT, security, or risk and compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

Figure 6

"Do you feel the consequences of these security breaches are becoming more or less challenging to deal with than they were a year ago?"



Base: (Varies by variable) IT, security, or risk and compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

Hardware Security Vendors Are Key To Reducing Threats

Those with a more focused hardware-level security approach are better prepared to fend off threats, but even they can do more with the proper hardware security vendor. Companies are already looking to outsource their security measures to vendor services that can front the load of securing the BIOS and hardware supply chain. However, not all vendors are regarded as equal.

› **Hardware-level security practices are still maturing.** Chip manufacturer validation and supply chain validation are viewed as the most salient initiatives for addressing threats at the BIOS and hardware-level. Firms have pledged to embrace more security practices in the coming months. Many have already begun adopting and investing in supply chain validation initiatives: 47% are implementing now and 30% plan to implement in the next 12 months. Chip manufacturer validation is a security initiative that, although not in use now, is the initiative that most firms are planning to adopt in the next year, with 38% pledging to do so.

Biggest challenge in securing the hardware supply chain:

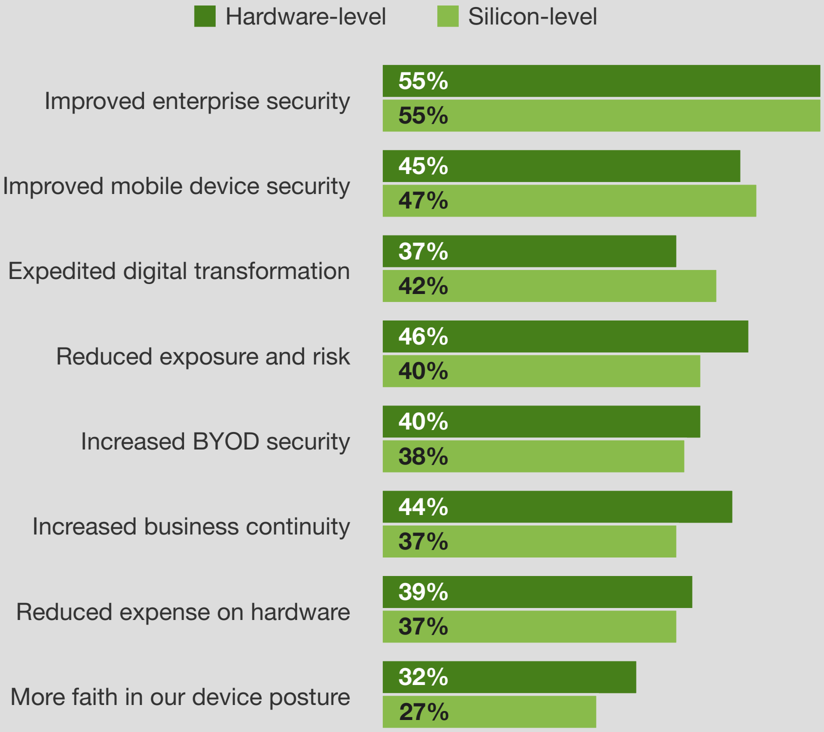
"Our **BYOD policy** needs to be more stringent. **Chip validation** must be implemented to protect against ransomware attacks. . . . **We also have a hard time** finding the **right vendors** to work with on a long-term basis."

IT, security manager, at an enterprise in Germany

- **Securing hardware and silicon levels result in huge benefits across the organization.** Those that invest in stronger security measures see improvements across many vectors. Organizations report growth in their enterprise's overall security (55%), reduced expenses to their hardware (39%), increased business continuity (44%), and expedited digital transformation (42%) (see Figure 7).
- **The right hardware security vendor is crucial to securing the supply chain.** Endpoint security and platform security are both equally important features that are expected from hardware security vendors by 61% percent of organizations. Over half see security at the silicon level and throughout the supply chain as a standard in service (55% and 58%, respectively). Although firms expect top-notch security from their vendors, only 28% of firms said they were satisfied with the device security practices their vendor provided at the silicon level.

Figure 7

"What benefits have you achieved, or do you expect to achieve, as a result of securing your hardware or silicon levels?"



Base: 307 IT, security, or risk & compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

Key Recommendations

As security decision makers look to modernize and secure their technology, they should focus on validating their hardware and firmware and allowing trusted vendors to scaffold the brunt of keeping BIOS protected. The first part of of doing that is understanding where your hardware has come from, who's produced it — and how much trust you can put into that provider or vendor.

Forrester's in-depth online survey of 307 IT, security, risk, and compliance decision makers at companies with more than 500 employees yielded several important recommendations:

What you buy and who you buy it from matters greatly. Hardware — and its silicon infrastructure — is the core component of all computing systems. They literally cannot function without it, and every endpoint on the planet relies on it. The origins and handling of these components and the finished products — notably who produced it and where — can make the difference between a trusted device free of tampering and one that contains a latent threat which may only surface once the endpoint is in use. It's critical to be fully cognizant of the supply chain, from component manufacture through assembly and transport to your site and ensure that your vendor can attest to the security of their components from the production floor all the way to your office.

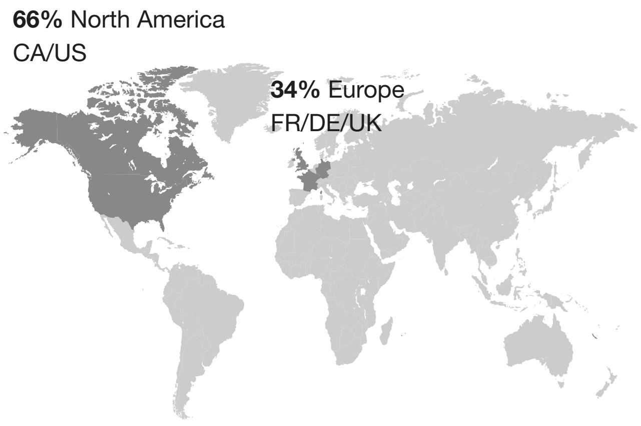
BIOS is prime territory today for cyber-attacks — and securing your Firmware is a fundamental step in defense. Because organizations have long deployed and managed technologies for virus detection, encryption and other 'above the OS' defenses, attackers are now seeking easier targets in the endpoint hardware: notably the BIOS. Make sure you have solutions in place that enable the detection of BIOS and boot level anomalous activities, to engage defenses against them. If you don't, you may be missing stealthy attacks which can do immense damage to your organization. Ignorance in the cyber arena is never bliss.

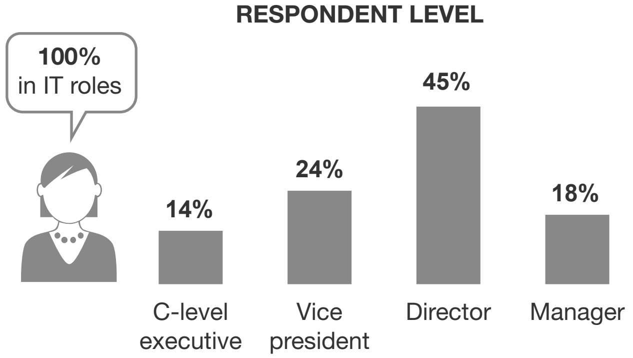
BIOS and hardware level exploitation is designed to evade your typical enterprise security controls. The reality is that if a machine boots up with a BIOS contaminated by a stealthy attack, normal detection methods and defensive measures won't stop it from wreaking havoc. Be pragmatic about the realities of this type of threat and understand and communicate the truth about these exploits to those that procure your enterprise computing solutions. When the future of your company is at stake, validated and secure hardware and firmware including BIOS — from a trusted vendor can keep your organization running efficiently.

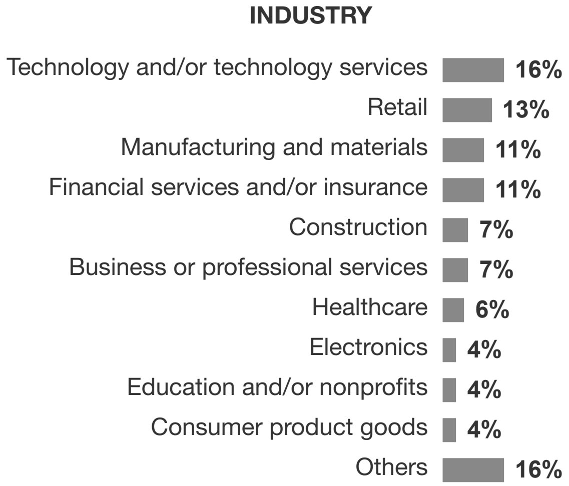
Appendix A: Methodology

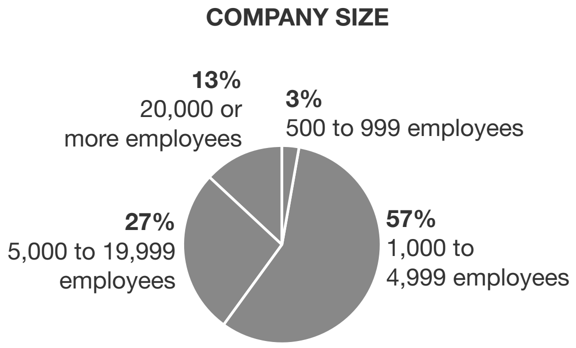
In this study, Forrester conducted an online survey of 307 enterprises in the United States, Canada, the United Kingdom, France, and Germany to evaluate the value of utilizing trusted devices to better protect company supply chains from hardware- and silicon-level data breaches. Survey participants included decision makers in IT, security, and risk and compliance roles at companies with more than 500 employees. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in March 2019 and was completed in May 2019.

Appendix B: Demographics









Base: 307 IT, security, or risk and compliance decision makers (manager level and above) in North America and Europe
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, April 2019

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

"Unified Endpoint Management (UEM) Finally Arrives," Forrester Research, Inc., January 18th, 2018.

"Top Cybersecurity Threats In 2019," Forrester Research, Inc., December 11th, 2018.