



CRITICAL  
CYBER  
THREAT

SUPER MICRO  
SUPERNOVA

Houston,  
we have a  
problem!

Mercury Systems Inc. | NASDAQ: MRCY

INVESTMENT RESEARCH REPORT

*"Cyber Systems Failure"*

RECOMMENDATION: *Strong Sell Opinion*

This research presentation expresses our research opinions. You should assume that as of the publication date of any presentation, report or letter, Spruce Point Capital Management LLC (possibly along with or through our members, partners, affiliates, employees, and/or consultants) along with our subscribers and clients has a short position in all stocks (and are long/short combinations of puts and calls on the stock) covered herein, including without limitation Mercury Systems, Inc. (“MRCY”), and therefore stand to realize significant gains in the event that the price of its stock declines. Following publication of any presentation, report or letter, we intend to continue transacting in the securities covered therein, and we may be long, short, or neutral at any time hereafter regardless of our initial recommendation. All expressions of opinion are subject to change without notice, and Spruce Point Capital Management does not undertake to update this report or any information contained herein. Spruce Point Capital Management, subscribers and/or consultants shall have no obligation to inform any investor or viewer of this report about their historical, current, and future trading activities.

This research presentation expresses our research opinions, which we have based upon interpretation of certain facts and observations, all of which are based upon publicly available information, and all of which are set out in this research presentation. Any investment involves substantial risks, including complete loss of capital. Any forecasts or estimates are for illustrative purpose only and should not be taken as limitations of the maximum possible loss or gain. Any information contained in this report may include forward looking statements, expectations, pro forma analyses, estimates, and projections. You should assume these types of statements, expectations, pro forma analyses, estimates, and projections may turn out to be incorrect for reasons beyond Spruce Point Capital Management LLC’s control. This is not investment or accounting advice nor should it be construed as such. Use of Spruce Point Capital Management LLC’s research is at your own risk. You should do your own research and due diligence, with assistance from professional financial, legal and tax experts, before making any investment decision with respect to securities covered herein. All figures assumed to be in US Dollars, unless specified otherwise.

To the best of our ability and belief, as of the date hereof, all information contained herein is accurate and reliable and does not omit to state material facts necessary to make the statements herein not misleading, and all information has been obtained from public sources we believe to be accurate and reliable, and who are not insiders or connected persons of the stock covered herein or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer, or to any other person or entity that was breached by the transmission of information to Spruce Point Capital Management LLC. However, Spruce Point Capital Management LLC recognizes that there may be non-public information in the possession of MRCY or other insiders of MRCY that has not been publicly disclosed by MRCY. Therefore, such information contained herein is presented “as is,” without warranty of any kind – whether express or implied. Spruce Point Capital Management LLC makes no other representations, express or implied, as to the accuracy, timeliness, or completeness of any such information or with regard to the results to be obtained from its use.

This report’s estimated fundamental value only represents a best efforts estimate of the potential fundamental valuation of a specific security, and is not expressed as, or implied as, assessments of the quality of a security, a summary of past performance, or an actionable investment strategy for an investor. This is not an offer to sell or a solicitation of an offer to buy any security, nor shall any security be offered or sold to any person, in any jurisdiction in which such offer would be unlawful under the securities laws of such jurisdiction. Spruce Point Capital Management LLC is not registered as an investment advisor, broker/dealer, or accounting firm.

**All rights reserved. This document may not be reproduced or disseminated in whole or in part without the prior written consent of Spruce Point Capital Management LLC.**



## *Executive Summary*

## *Spruce Point Reiterates 50%-60% Downside Risk In Mercury Systems Based On New Findings*

Spruce Point finds evidence to suggest that Mercury Systems (Nasdaq: MRCY) could be one of the companies affected by the alleged Super Micro Computer, Inc. (Supermicro) hack, and can demonstrate recent actions taken by management to obscure the relationship. We believe the Street is structurally misunderstanding the magnitude of the revenue delays and cyber compliance costs that Mercury – a company presently without a Chief Information Security Officer (“CISO”) – will face going forward. Based on our expert calls, we expect that cybersecurity-related costs could mount to 10% of revenues. Given that management felt it necessary to hide its relationship with Supermicro, we believe that Mercury needs to disclose to investors the materiality of its exposure to Supermicro components, the financial impact of any product changes/recalls/replacements, and its plans to ensure the “security” of its mission-critical products on a go-forward basis.

### **Exposure Emanating From “Technology Partner” Supermicro**

- On October 4<sup>th</sup>, [Bloomberg published an in-depth article](#) highlighting how China infiltrated 30 U.S. companies by inserting a tiny chip into Supermicro motherboards. Navy systems were mentioned specifically as an affected target. Mercury Systems and two of its recent acquisitions – Themis Computers (\$175 million / Feb 2018) and Germane Systems (\$45 million / July 2018) – each sells servers and other related IT equipment containing Supermicro motherboards to the Navy and other military branches.
- Providing secure and resilient solutions to prime and government customers is the essence of Mercury's business. Mercury mentions the words “secure” and “security” over 100 times in its annual report.
- Mercury, Themis, and Germane all listed Supermicro as a “technology partner” on their respective websites until last week, when nearly all references to the relationship were abruptly and surreptitiously removed between October 8-9 without explanation.
- The existence of Supermicro motherboards in Mercury’s rugged servers presents difficult-to-quantify tail risks, but could force product recalls and expensive supply chain adjustments, among other costly actions. As a precedent example, the Navy placed restrictions on IBM’s BladeCenter server line in 2015 over supply chain security concerns, less than a year after Chinese IT hardware manufacturer Lenovo acquired IBM’s server business. ([USNI Article](#))

### **Cyber Compliance Is Likely To Drag On Revenue Growth And Materially Increases Costs**

- A recent GAO report entitled [“DOD Just Beginning to Grapple with Scale of Vulnerabilities”](#) highlighted how testers playing the role of adversary were able to take control of systems relatively easily and operate largely undetected. Based on conversations with industry experts, we believe that the requirements for winning government business will be (and are being) rewritten with an emphasis on cyber resilience and a much higher cybersecurity standard. We suspect that new contracts awards are likely to be delayed as a result. 4

# *Spruce Point Reiterates 50%-60% Downside Risk In Mercury Systems Based On New Findings*

- Based on our research, Mercury appears ill-prepared to address these new requirements given its relative shortage of cybersecurity personnel, and the fact that both its long-time CIO and long-time CISO recently departed in August 2018. We estimate that Mercury could have to spend up to 10% of revenue on cyber-related costs going forward, or otherwise make a costly acquisition to comply with these new customer expectations.
- Mercury has quietly hinted at some of these concerns through subtle changes to its 10-K risk factors and safe harbor provisions, and through recent job postings in supply chain procurement and quality control.
- On October 8<sup>th</sup>, Mercury introduced “50 Models To Its Rugged Server Product Line”- could this be a tacit admission of problems?

## **Deteriorating Financial Metrics, Undisclosed Signs Of Strain, And Evidence Of Misrepresentation**

- In our first report, we highlighted Mercury’s risk of losing its small business status for government contracts. Mercury lost this status earlier this year, which has coincided with rising inventories relative to backlog convertible to revenues in the next 12 months.
- Mercury’s gross margins have now fallen below its “low target” of 45%, and could compress further due to Defense Federal Acquisition Regulations Supplement (DFARS) compliance issues and potential product recall costs from the Supermicro fallout.
- Additionally, Mercury recently amended its credit agreement for a third time in late September 2018, but never disclosed that it had amended the agreement previously in December 2017, just as it began factoring accounts receivable. Factoring accounted for a substantial 43% of FY18 operating cash flow.

## **Mercury’s Irrational Valuation Multiple Could Materially Contract**

- Mercury currently has the highest valuation in the Aerospace & Defense industry despite posting the sector’s weakest cash flow as a percentage of revenue and average organic revenue growth.
- Sell-side analyst see just 9.5% upside in its share price, but haven’t factored in complications arising from its Supermicro relationship and rising cyber compliance costs.
- Taking these issues into consideration, and discounting Mercury’s multiple to the industry average, we estimate 50%-60% downside.

Mercury's stock has risen in recent months due to increased government defense spending and the accelerated speed with which contracts are being awarded. The Themis/Germane acquisitions appeared to position Mercury to benefit from \$100m of additional revenue (~16% of FY 2019E revenue). However, the Street is ignoring a host of fundamental red flags in Mercury's filings, near-term tail risks stemming from its relationship with Supermicro, and the longer-term implications of rising cybersecurity costs.

## Red Flags From Mercury's SEC Filings

- Additional language added to Mercury's 10-K risk factors and safe harbor provision regarding cybersecurity, compliance costs
- Warranty accruals as a % of sales have rapidly declined, which could indicate future earnings overstatement
- Mercury finally lost its designation as a "small business" contractor
- Cash flow conversion remains anemic and increased in Q4 primarily due to inventory accounting changes made after our critical report, raising concerns that management pulled levers in a fleeting attempt to deflect longer-term challenges. In particular, Mercury resorted to factoring receivables in FY 2018 to pull forward cash flow.
- Gross margins continue to fall well below its 50% target; mgmt. blames recent acquisitions as having lower margins
- Mercury's inventory and planned inventory purchases remain historically elevated relative to its next 12 months backlog to be shipped. Next 12 months backlog to be shipped relative to total backlog is at its lowest level in 6 years.
- Insider ownership is at a record low, while insiders continue to sell post our critical report in April

## Potential Near-Term Supermicro Implications

- Product recalls and any charges or costs to the income statement attributable to inventory obsolescence or rising warranty claims
- Costs associated with new product introductions to replace motherboards, including sales, marketing, and educating customers about the product changes
- Ability to hit near-term quarterly sales and earnings targets may suffer

## Potential Long-Term Cybersecurity Implications

- Additional margin compression due to increased long-term costs related to cybersecurity monitoring and supply chain auditing
- Mercury has neither the executives nor human talent in place to address the growing cybersecurity threat. Hiring of technical IT talent and/or external consultants versed in cybersecurity will materially increase costs.
- **Experts we have spoken to suggest costs could rise up to 10% of revenues due to emerging cybersecurity demands**
- Ability to hit long-term financial targets may suffer and multiples may contract due to the business' changing cost structure
- Loss of business relationships
- Shareholder lawsuits

**We believe owning Mercury at the current price is a terrible risk/reward proposition. The average analyst price target of ~\$56/share implies just 9.5% upside, when not a single analyst is questioning the implications of replacing a key technology partner.**

**We believe Mercury remains the most expensive stock in the A&D sector with 50%-60% downside risk.**

# *Spruce Point Estimates 50%-60% Downside Risk*

We believe the Street is structurally misunderstanding the magnitude of the cybersecurity-related costs that Mercury will face going forward, as well as the delays in revenue contract award opportunities it will face in its high-growth “command, control, communications, computers, and intelligence” (C4I) segment – expected to be a \$100m business. Mercury does not even have a CISO at present, and only recently replaced its departed CIO.

\$ in millions, except per share amounts

Valuation	Best Case Price	Worst Case Price	Note
<p><b>Sales Multiple</b></p> <p>CY Street 2019E Sales</p> <p><u>Spruce Point Adjusted</u></p> <p>Enterprise Value</p> <p>Plus: Cash</p> <p>Less: Debt</p> <p><u>Dil. Shares</u></p> <p>Price Target</p> <p>% Downside</p>	<p>2.0x</p> <p>\$645.8</p> <p><u>\$635.8</u></p> <p>\$1,272</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$23.12/sh</b></p> <p>-55%</p>	<p>2.0x</p> <p>\$645.8</p> <p><u>\$630.8</u></p> <p>\$1,262</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$22.91/sh</b></p> <p>-56%</p>	<ul style="list-style-type: none"> <li>Mercury has suggested that its Themis / Germane business will add \$100m of revenues, but with its recent removal of its tech partnership with Supermicro – which it says supports “short lead times” – there is bound to be slippage to revenue expectations</li> <li>Furthermore, we expect the added burden of having to comply with new DFARS regulations to delay contract awards. Mercury must now certify its cybersecurity requirements.</li> <li>Our worst case assumes Mercury achieves 85% of run rate revenues, and base case assumes 90% of its C4I rugged server expectations</li> <li>Mercury trades at 4x sales vs. the industry at 2x. Given serious security overhangs, Mercury’s multiple should compress to the industry average.</li> </ul>
<p><b>Multiple of EBITDA</b></p> <p>CY Street 2019E EBITDA</p> <p><u>Spruce Point Adjusted</u></p> <p>Enterprise Value</p> <p>Plus: Cash</p> <p>Less: Debt</p> <p><u>Dil. Shares</u></p> <p>Price Target</p> <p>% Downside</p>	<p>12.5x</p> <p>\$146</p> <p><u>\$114</u></p> <p>\$1,425</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$26.35/sh</b></p> <p>-49%</p>	<p>12.5x</p> <p>\$146</p> <p><u>\$83</u></p> <p>\$1,037</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$18.20/sh</b></p> <p>-65%</p>	<ul style="list-style-type: none"> <li>We layer in additional long-term costs for the new DFARS cybersecurity compliance requirements</li> <li>Our industry expert with 30yrs+ experience working with major primes in contracting and compliance believes that companies like Mercury should be prepared to absorb up to 10% of revenues to deal with new regulatory requirements. We model this as a worst case outcome, and 5% as base case</li> <li>In the event that Mercury acquires a cybersecurity company rather than develop needed cybersecurity capabilities in-house, it would effectively be capitalizing the cost with no revenue benefit, and with incremental interest expense cost</li> <li>Peer average multiple of 12.5x</li> </ul>
<p><b>Multiple of EPS</b></p> <p>CY Street 2019E EPS</p> <p><u>Spruce Point Adj EPS</u></p> <p>Price Target</p> <p>% Downside</p>	<p>18.0x</p> <p>\$1.84</p> <p><u>\$1.07</u></p> <p><b>\$19.26</b></p> <p>-63%</p>	<p>18.0x</p> <p>\$1.84</p> <p><u>\$0.54</u></p> <p><b>\$9.79</b></p> <p>-81%</p>	<ul style="list-style-type: none"> <li>Depreciation and Amortization of \$41.5m</li> <li>Tax rate of 20%</li> <li>Interest expense of \$9.6m (\$240m @ 3.9%)</li> <li>Peer average multiple of 18x</li> </ul>

# Time Line of Shady Events

The chain of events leading up to the recent news of the alleged Supermicro espionage is cause for concern.

2017				2018							
Aug	Sept	Oct	Dec	Feb	April	May	June	July	Aug	Sept	Oct
Insiders Enact Stock Sale Program	Chief Acct'g Officer Resigns	Adds Mention of Cybersecurity Regulations and Costs To Safe-Harbor Provision	Themis Deal Announced	Closes Themis Deal	Spruce Point Issue Critical Strong-Sell Report	Richard Jaenicke Director of Strategic Marketing and Alliances Leaves Sometime After May		Reports Q4'18 Results	CIO and CSIO leave Mercury	Discloses new Gov't Relations Board Committee Formed in 2017	Mercury Discloses 3 <sup>rd</sup> Credit Agreement Amendment (Never Disclosed the 2 <sup>nd</sup> )
Severance Terms Changed For CEO And Executives			Mercury Fails To Disclose 2 <sup>nd</sup> Credit Agreement Amendment	CFO Gerald Haines Resigns After 10-Q Filed				Acquires Germane Systems	Filed 10-K Discloses It Lost "Small Business" Status		Bloomberg Breaks Supermicro Hack Story
Disclosed It Could Lose "Small Business" Designation	Adds Method For Reporting Fraud In Proxy St		Mercury Fails To Disclose It Factored Receivables						10-K Risk Factors on Cyber-security And Compliance Cost Changed		Mercury Removes Supermicro From Websites
											Posts New Jobs For "Snr. Quality Manager" and "Manager, Supply Chain"

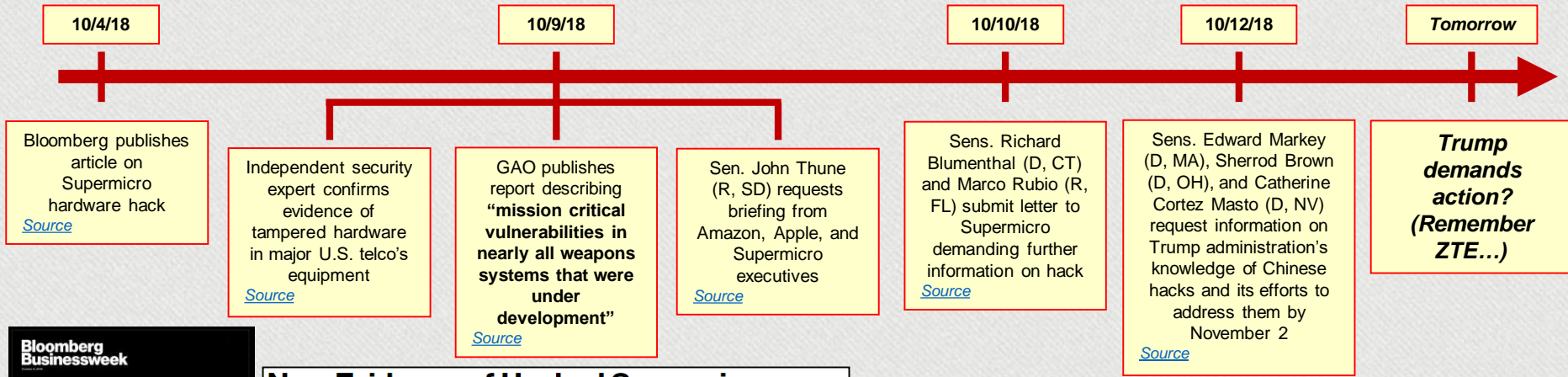




*Background On Supermicro Hack  
And Growing Concerns Regarding  
Supply Chain Vulnerabilities*

# Prospect Of Supermicro Hardware Hack Has Potential To Spur Near-Term Industry Change

Military cybersecurity is still a nascent field, and some assume that it will take time for firms to integrate relevant technologies into their products, or to shift their supply chains away from at-risk sources. However, the prospect of a Supermicro hardware hack could force affected hardware providers to act on these threats within a very short timeframe, as authorities and the public have taken notice of the threat.



**New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom**

The discovery shows that China continues to sabotage critical technology components bound for America.

By [Jordan Robertson](#) and [Michael Riley](#)  
October 9, 2018, 11:01 AM EDT Updated on October 9, 2018, 5:37 PM EDT

**GAO Highlights**

October 2018  
**WEAPON SYSTEMS CYBERSECURITY**  
DOD Just Beginning to Grapple with Scale of Vulnerabilities

We found that from 2012 to 2017, DOD testers routinely found mission-critical cyber vulnerabilities in nearly all weapon systems that were under development. Using relatively simple tools and techniques, testers were able to take control of these systems and largely operate undetected. In some cases, system operators were unable to effectively respond to the hacks. Furthermore, DOD does not know the full scale of its weapon system vulnerabilities because, for a number of reasons, tests were limited in scope and sophistication.

[Source](#)

With public awareness of the Chinese hack story high, relations with China cooling, and military spending cycles accelerated under the Trump administration, it would be no surprise if the government encouraged domestic sourcing or other remedial actions for companies tied to Supermicro within a relatively short period of time, forcing companies like Mercury to bring forward their cybersecurity-related spending rapidly.

# Companies Posing Military Supply Chain Risks Have Been Punished By The Military And The Market

There is precedent for military branches to act on sudden, demonstrated supply chain risks in short order: in May 2015, seven months after IBM sold its server division to Chinese hardware manufacturer Lenovo, the Navy placed restrictions on purchases of IBM/Lenovo BladeCenter products, and initiated a search for a new server provider for its Aegis Combat System. The DoD continues to issue warnings regarding potential Lenovo M&A of U.S. military IT providers.

## U.S. Navy Looks to Replace IBM Servers for Security After Lenovo Purchase

Department of Homeland Security identifies security concerns with IBM unit sale

By Eva Dou

Updated May 19, 2015 3:49 p.m. ET

**Navy announcement of Lenovo concerns coincides almost precisely with the peak in Lenovo's share price**

## Lenovo's Share Price Never Recovered After The Supply Chain Risk



Though a weak Chinese smartphone market and slowing global PC demand were also responsible for the pullback in Lenovo shares, supply chain-related security concerns regarding the sale of IBM's server business to a Chinese company were also cited as a reason for poor share performance at the time ([Source](#))

# Supermicro Denial Not Believed By The Market Based On Share Price

Supermicro has denied allegations of a security breach, but the company's share price suggests that the market is skeptical of management's defense.<sup>1</sup> According to Bloomberg, an independent security expert detected a Supermicro-related hardware intrusion at a U.S. telecom company several days after concerns were first raised about Supermicro, but the hack was of a different variety than that described by the initial Bloomberg report.<sup>2</sup>

Coincidentally, Mercury's CISO and CIO both left the firm in August 2018 – just before the story broke – and Mercury subsequently removed nearly all references to Supermicro from its website (see forthcoming slides).



Source: Bloomberg

- 1) "Supermicro Refutes Claims In Bloomberg Article", [press release](#), Oct 4, 2018
- 2) "New Evidence of Hacked Supermicro Hardware Found In U.S. Telecom", [Bloomberg](#), Oct 9, 2018
- 3) Based on Mercury's CISO's and CIO's LinkedIn biographies [here](#) / [here](#)



*Evidence Of Cybersecurity  
Challenges At Mercury Following  
Supermicro News*

The word "security" appears 61 times, and the word "secure" 45 times, in Mercury's FY 2018 10-K

## Our Business Strategy

Our strategy is built around our key strengths as a leading commercial provider of secure sensor and safety critical mission processing subsystems. Optimized for customer and mission success, our solutions power a wide variety of critical defense and intelligence programs. We are pioneering a next-generation defense electronics business model specifically designed to meet the industry's current and emerging technology needs. By driving this strategy consistently, we are able to help our customers, mostly defense prime contractors, reduce program cost, minimize technical risk, and stay on schedule and on budget. Tactically, we have a reputation of relentless execution on behalf of our customers that supports the successful evolution of our strategy.

We intend to accelerate our strategic direction through continued investment in advanced new products and solutions development in the fields of radio frequency, analog-to-digital and digital to analog conversion, advanced multi- and many-core sensor processing systems including GPUs, embedded security, digital storage, and digital radio frequency memory ("DRFM") solutions, software defined communications capabilities, and advanced security technologies and capabilities. We leverage our engineering development capabilities including systems integration to accelerate our move to become a commercial outsourcing partner to the large defense prime contractors as they seek the more rapid design, development and delivery of affordable, commercially developed, open sensor processing solutions within the markets we serve. We invest in scalable manufacturing operations in the U.S. to enable rapid, cost-effective deployment of our microelectronics and secure processing solutions to our customers. Our engagement model can help lead to long-term production subsystem revenues that will continue long after the initial services are delivered.

This business model positions us to be paid for non-recurring engineering work we would have previously expensed through our own income statement, to team concurrently with multiple defense prime contractors as they pursue new business with the unique solutions they develop and market to the government, and to engage with our customers much earlier in the design cycle and ahead of our competition. Since July 2015, we have substantially added to our technology portfolio by adding capabilities in embedded security with the acquisitions of Lewis Innovative Technologies ("LIT") and the custom microelectronics, RF and microwave solutions, and embedded security operations of Microsemi Corporation (the "Carve-Out Business"), RF solutions and custom microelectronics solutions with the acquisitions of the Carve-Out Business and Delta Microwave, LLC ("Delta"), mission computing, safety-critical avionics and platform management with the CES Creative Electronic Systems, S.A. ("CES") and Richland Technologies, LLC ("RTL") acquisitions, and rugged servers, computers and storage systems with the acquisitions of Themis Computer ("Themis") and Germane Systems, LC ("Germane").

Our deep domain knowledge within our company rounds out our capabilities and services to our prime contractor and DoD customers. The acquisitions of the Carve-Out Business and Delta further improved our ability to compete successfully in these market segments by allowing us to offer an even more comprehensive set of closely related capabilities. The CES and RTL acquisitions provided us new capabilities that substantially expand our addressable market into commercial aerospace, defense platform management and mission computing markets that are aligned to our existing market focus. The additions of Themis and Germane provide us with new capabilities and position us with a significant footprint within the C2I rugged server business.

- *Diverse Mix of Stable, Growth Programs Aligned with DoD Funding Priorities.* Our products and solutions have been deployed on more than 300 different programs and over 25 different defense prime contractors. We serve high priority markets for the DoD and foreign militaries, such as UAVs, ballistic missile defense, guided missiles and precision munitions, airborne reconnaissance, EW, and have secure positions on mission-critical programs including Aegis, Predator and Reaper UAVs, F-35 Joint Strike Fighter, Patriot missile, SEWIP, and Paveway. In addition, we consistently leverage our technology and capabilities across multiple programs, providing significant operating leverage and cost savings. Our recent acquisitions allow us to participate in a broader array of programs, many with customers that are already key strategic customers of ours.
- *We are a leading commercial provider of secure processing subsystems designed and made in the U.S.A.* We have a portfolio of open standards architecture ("OSA") technology building blocks across the entire sensor processing chain. We offer embedded secure processing capabilities with advanced packaging and cooling technologies that ruggedize commercial technologies while allowing them to stay cool for reliable operation. These capabilities allow us to help our customers meet the demanding SWaP requirements of today's defense platforms. Our pre-integrated subsystems improve affordability by substantially reducing customer system integration costs and time-to-market for our solutions. System integration costs are one of the more substantial costs our customers bear in developing and deploying technologies in defense programs and platforms. Our pre-integrated solutions approach allows for more rapid and affordable modernization of existing platforms and faster deployment of new platforms.

Our strengths in this area include our position as an early and leading advocate for OSA in defense, offering Intel server class processing form factors across 3/6U OpenVPX, ATCA and rack-mount architectures, and high density, secure solutions across multiple hardware architectures to seamlessly scale to meet our customers' SWaP requirements. In addition, we have a 30-year legacy of system management and system integration expertise that allows us to reduce technical risk, while improving affordability and interoperability. Our system integration expertise is a cornerstone in helping us support our customers in deploying pre-integrated, OSA subsystems.

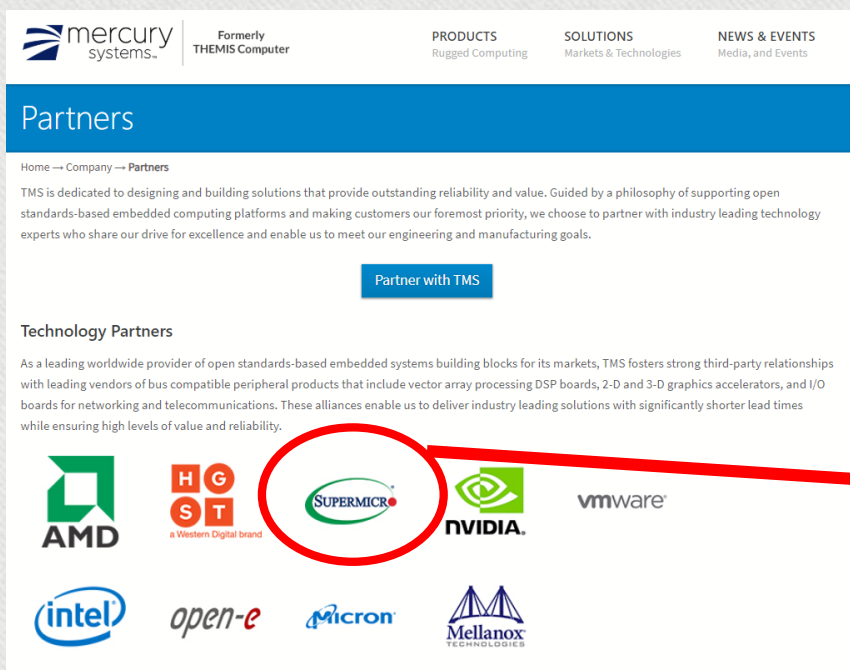
- *We provide advanced, integrated security features for our products and subsystems, addressing an increasingly prevalent requirement for DoD program security.* We offer secure processing expertise that is built-in to our pre-integrated subsystems, not bolted on. By doing this we are able to provide secure building blocks that allow our customers to also incorporate their own security capabilities. This assists our customers in ensuring program protection as they deploy critical platforms and programs, all in support of DoD missions. The Carve-Out Acquisition brought us new security technologies and also allowed us to provide enhanced security capabilities in areas such as memory and storage devices. The Carve-Out Acquisition also provided us

# Mercury Obfuscating Relationship With Supermicro After The Bloomberg Report

Themis and Mercury's relationship with Supermicro was so strong that it was listed as one of their nine technology partners. However, following the Bloomberg report, Mercury quietly removed Supermicro as a partner from its website.

Given that Mercury cites the relationship as allowing it to deliver solutions with *“significantly shorter lead times while ensuring high levels of value and reliability,”* the loss of Supermicro as a technology partner will, at a minimum, cause short-term – and perhaps long-term – disruptions to the business. Mercury needs to address the impact of the lost partnership with investors, in addition to the describing the remedies which it may have to undertake to address potential security risks in both existing inventory and servers in the field.

## Prior To October 8, 2018



mercury systems. Formerly THEMIS Computer

PRODUCTS Rugged Computing SOLUTIONS Markets & Technologies NEWS & EVENTS Media, and Events

### Partners

Home → Company → Partners

TMS is dedicated to designing and building solutions that provide outstanding reliability and value. Guided by a philosophy of supporting open standards-based embedded computing platforms and making customers our foremost priority, we choose to partner with industry leading technology experts who share our drive for excellence and enable us to meet our engineering and manufacturing goals.

[Partner with TMS](#)

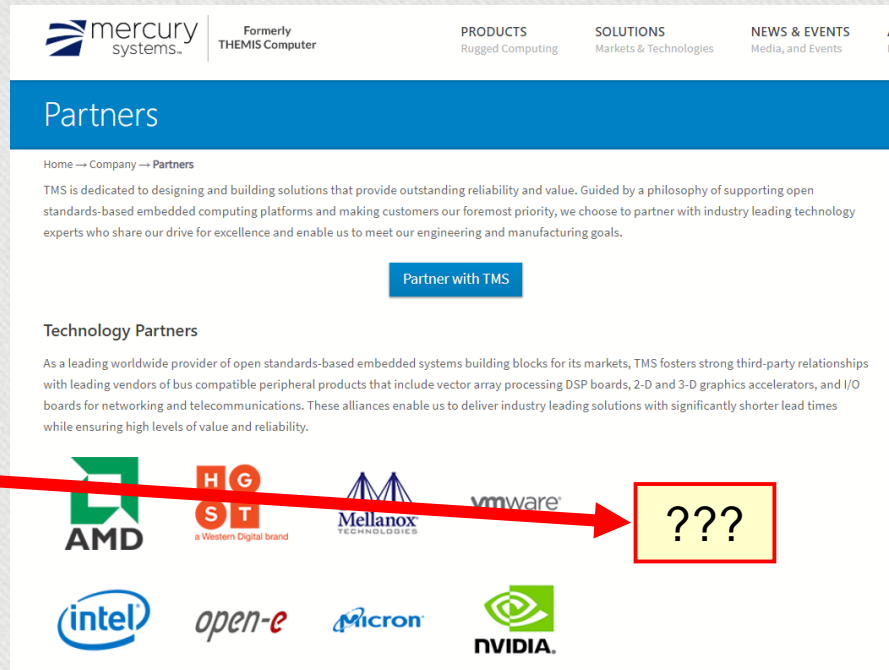
#### Technology Partners

As a leading worldwide provider of open standards-based embedded systems building blocks for its markets, TMS fosters strong third-party relationships with leading vendors of bus compatible peripheral products that include vector array processing DSP boards, 2-D and 3-D graphics accelerators, and I/O boards for networking and telecommunications. These alliances enable us to deliver industry leading solutions with significantly shorter lead times while ensuring high levels of value and reliability.

Logos: AMD, HGST, SUPERMICRO, NVIDIA, vmware, intel, open-e, Micron, Mellanox

Source: Mercury/Themis [cached website](#) (10/2/2018) (archived [here](#))

## After October 8, 2018



mercury systems. Formerly THEMIS Computer

PRODUCTS Rugged Computing SOLUTIONS Markets & Technologies NEWS & EVENTS Media, and Events

### Partners

Home → Company → Partners

TMS is dedicated to designing and building solutions that provide outstanding reliability and value. Guided by a philosophy of supporting open standards-based embedded computing platforms and making customers our foremost priority, we choose to partner with industry leading technology experts who share our drive for excellence and enable us to meet our engineering and manufacturing goals.

[Partner with TMS](#)

#### Technology Partners

As a leading worldwide provider of open standards-based embedded systems building blocks for its markets, TMS fosters strong third-party relationships with leading vendors of bus compatible peripheral products that include vector array processing DSP boards, 2-D and 3-D graphics accelerators, and I/O boards for networking and telecommunications. These alliances enable us to deliver industry leading solutions with significantly shorter lead times while ensuring high levels of value and reliability.

Logos: AMD, HGST, Mellanox, vmware, intel, open-e, Micron, NVIDIA, and a placeholder '???' in a yellow box.

Source: Mercury/Themis current [website](#) (archived [here](#))

# Mercury / Germane Systems Obfuscate Supermicro Relationship

Germane Systems – Mercury’s other recent acquisition in the command, control & intelligence (C2I) space – also touts a technology partnership with Supermicro, and has even retweeted Supermicro product announcements. Recent Germane Systems product spec sheets also reference Supermicro motherboards.

Mercury just deleted references to Supermicro as a technology partner on Germane’s website.

## Morning of October 9, 2018

Technology Partnerships



Source: Germane Systems “About Us”, [cached version](#) (8/23/2018) (archived in original form [here](#)). Also see earlier archived version [here](#) with reference to Supermicro.

## Afternoon of October 9, 2018

Technology Partnerships



Source: Germane Systems “About Us” [website](#) (archived [here](#))

## Germane Systems Product Spec Includes Supermicro

DESIGN | TEST | BUILD | SUPPORT



### GRS-3410G STORAGE SERVER SPECIFICATIONS

#### Processors and Motherboards

- Dual Intel® Xeon® E5-2600 V3/V4 processors
  - up to 22 cores per CPU with 9.6GT/s QPI
- Supermicro X10DRI-T motherboard
  - Optional motherboards available
- Supports various O/S (including Ubuntu, Red Hat, Microsoft and others)

#### Rear I/O

- 6 PCIe 3.0 full height slots
  - 3x PCIe X16 slots and 3x PCIe X8 slots
- PS2 keyboard and mouse connectors
- 4 USB 3.0 ports
- VGA Graphics port
- 1 IPMI 2.0 port (optional)

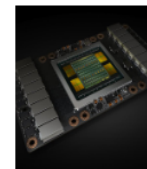
Source: Germane Systems [Product Spec](#)

## Germane Systems Retweets Supermicro (9/27/2017)

Germane Systems Retweeted

Supermicro @Supermicro\_SMCI · 27 Sep 2017

#GPU Optimized Systems for @nvidia Tesla V100 GPUs. Read the #pressrelease here [supermicro.com/newsroom/press...](http://supermicro.com/newsroom/press...)



NVIDIA Data Center @NVIDIADC

.@DellEMC, @HPE, @IBMPowerSystems and @Supermicro\_SMCI announced servers based on NVIDIA Tesla #V100 GPUs. [nvda.ws/2ythElo](http://nvda.ws/2ythElo)

5 11

Source: Germane Systems [Twitter](#) (direct link to tweet [here](#), archived [here](#))



# Are “New Products” Really Just A Disguised Product Recall And Admission Of Hacked Products?

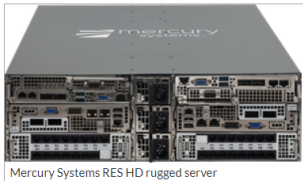
Immediately after removing references to Supermicro on its website, Mercury issued a press release on October 8 stating its plans to add over 50 models to its Enterprise Series rugged rackmount server product line. We find the timing of this announcement suspicious.

By visiting Mercury’s re-seller websites, we see that this series has historically incorporated Supermicro motherboards. Is this “new product launch” really a disguised recall meant to address the Supermicro threat without drawing attention to the issue?

## Timing of “50 Models Added” To Rugged Rackmount Server Line Is Suspicious

### Mercury Systems Adds Over 50 Models To Its Rugged Server Product Line

*Extends leadership in rackmount server market for defense applications*



ANDOVER, Mass., Oct. 08, 2018 (GLOBE NEWSWIRE) -- Mercury Systems, Inc. (NASDAQ: MRCY, [www.mrcy.com](http://www.mrcy.com)) announced it added more than 50 models to its EnterpriseSeries™ rackmount server product line, extending its leadership as one of the largest, most capable rugged rackmount server providers. Built from the ground up for mission critical applications where industry-leading performance, reliability, and SWaP are imperatives, Mercury’s servers are deployed in a variety of critical defense, industrial, and commercial applications.

“These new models in our EnterpriseSeries rackmount server line further expand Mercury’s capabilities in the C4ISR market,” said Scott Orton, Vice President and General Manager of Mercury’s Trusted Mission Solutions group. “We believe our knowledge and expertise in defense computing environments is second to none. With a multitude of form factors, configurations, and enhancement options – including nation-state-level security features – we can help our customers define the optimum server solution for their mission.”

Source: Mercury [press release](#)

## Rugged Rackmount Servers Have Incorporated Supermicro Motherboards



HOME ABOUT US PRODUCTS KEY PARTNERS SERVICES MEDIA CENTER CONTACTS

EuroLink Systems - Embedded Systems, Single Board Computer, FPGA, Data Acquisition, Drones > Products > Embedded Solutions > Avionics products > Mercury Rugged Rackmount Servers\_ Enterprise Series™

### PRODUCTS

#### Products Category

- Avionics products
- Boards
- Data Acquisition USB
- Display
- FPGA + DSP processing
- Industrial Networking
- Mass Storage
- Notebooks
- PC Box
- SBC
- SDR
- Server, Workstations & Panel PC
- Systems & Backplanes
- Tablet & PDA

### Mercury Rugged Rackmount Servers\_ Enterprise Series™

#### Main Features

Overview Specifications Gallery

#### Standard Density Servers

Available in 1U, 2U, and 3U, RIO and FIO form factors, and featuring E5-2600 v3/v4 Series Intel® Xeon® processors with up to twenty cores per socket, up to 1 TB DDR4 ECC memory, and enhanced reliability features, RES-XRS servers provide industry-leading performance and superior resilience to shock, vibration, and temperature extremes.

#### High Density Servers

Themis RES-HD Servers deliver high performance, double compute density, enable a 50% rack space savings, and reduce system weight by nearly 50%. Designed with leading edge components that include Intel® Xeon® E5-2600 v3 Series processors and **Supermicro motherboards**, RES-HD servers provide maximum system configuration flexibility and system expansion options with processor, storage, and system management module options.

Source: Eurolink [website](#) (archived [here](#))

**See the Appendix for further instances of Mercury wiping references to Supermicro from its website**

# Risk Factor Language Change Suggests Cybersecurity Is A Growing Concern For Mercury

Mercury recently expanded its risk factor language regarding “cyber intrusion” and “nation-state hackers”.

Mercury now warns that it must meet additional requirements to be awarded contracts, and that its compliance costs could increase.

New  
Language  
Added

**If we suffer any data breaches involving the designs, schematics, or source code for our products or other sensitive information, our business and financial results could be adversely affected.**

As a leading commercial provider to critical defense programs, our business may be subject to heightened risks of cyber intrusion as nation-state hackers seek access to technology used in U.S. defense programs. Like all DOD contractors that process, store or transmit controlled unclassified information, we must meet DFARS minimum security standards or risk losing our DOD contracts. We securely store our designs, schematics, and source code for our products as they are created. A breach, whether physical, electronic or otherwise, of the systems on which this sensitive data is stored could lead to damage or piracy of our products. If we are subject to data security breaches from external sources or from an insider threat, we may have a loss in sales or increased costs arising from the restoration or implementation of additional security measures, either of which could adversely affect our business and financial results. Other potential costs could include loss of brand value, incident response costs, loss of stock market value, regulatory inquiries, litigation, and management distraction. In addition, a security breach that involved classified information could subject us to civil or criminal penalties, loss of a government contract, loss of access to classified information, or debarment as a government contractor. Similarly, a breach that involved loss of customer-provided data could subject us to loss of a customer, loss of a contract, litigation costs and legal damages, and reputational harm.

The highly-publicized cyber-attack on Sony Pictures Entertainment demonstrates the vulnerability of companies to cyber-attacks and the severe impact these attacks can have. In addition to the potential costs discussed above, the Sony cyber-attack illustrates that such attacks can also damage physical infrastructure (e.g. corrupted servers) and destroy all copies of company intellectual property on a company's network.

Source: Mercury Systems FY 2018 [10-K](#) vs. FY 2017 [10-K](#)

New  
Language  
Added  
Elsewhere

“The new DFARS cybersecurity requirements may increase our costs or delay the award of contracts if we are unable to certify that we satisfy such cybersecurity requirements.”

# Safe Harbor Language Change Also Suggests Cybersecurity A Growing Issue

Looking carefully, we find that Mercury first added a reference to changes in “cybersecurity regulations and requirements” in its safe harbor statement on its Q1’17 earnings release (October 24, 2017). Just days earlier, on September 26, the Chief Accounting Officer resigned.<sup>1</sup> It is likely during this period that Mercury was conducting due diligence on Themis Computers, which it announced its intent to acquire on December 21.<sup>2</sup>

## Forward-Looking Safe Harbor Statement

This press release contains certain forward-looking statements, as that term is defined in the Private Securities Litigation Reform Act of 1995, including those relating to fiscal 2018 business performance and beyond and the Company's plans for growth and improvement in profitability and cash flow. You can identify these statements by the use of the words "may," "will," "could," "should," "would," "plans," "expects," "anticipates," "continue," "estimate," "project," "intend," "likely," "forecast," "probable," "potential," and similar expressions. These forward-looking statements involve risks and uncertainties that could cause actual results to differ materially from those projected or anticipated. Such risks and uncertainties include, but are not limited to, continued funding of defense programs, the timing and amounts of such funding, general economic and business conditions, including unforeseen weakness in the Company's markets, effects of continued geopolitical unrest and regional conflicts, competition, changes in technology and methods of marketing, delays in completing engineering and manufacturing programs, changes in customer order patterns, changes in product mix, continued success in technological advances and delivering technological innovations, changes in, or in the U.S. Government's interpretation of, federal export control or procurement rules and regulations, market acceptance of the Company's products, shortages in components, production delays due to performance quality issues with outsourced components, inability to fully realize the expected benefits from acquisitions and restructurings, or delays in realizing such benefits, challenges in integrating acquired businesses and achieving anticipated synergies, changes to cyber-security regulations and requirements increases in tax rates, changes to generally accepted accounting principles, difficulties in retaining key employees and customers, unanticipated costs under fixed-price service and system integration engagements, and various other factors beyond our control. These risks and uncertainties also include such additional risk factors as are discussed in the Company's filings with the U.S. Securities and Exchange Commission, including its Annual Report on Form 10-K for the fiscal year ended June 30, 2017. The Company cautions readers not to place undue reliance upon any such forward-looking statements, which speak only as of the date made. The Company undertakes no obligation to update any forward-looking statement to reflect events or circumstances after the date on which such statement is made.

New  
Language  
Added

Source: Mercury Systems Q1 2017 [Press Release](#)

- 1) Mercury's Chief accounting officer intends to resign, [8-K filing](#), Sept 26<sup>th</sup>, 2017
- 2) Mercury Systems To Acquire Themis Computers, [press release](#), Dec 21, 2017

# Mercury Does Not Have The Personnel To Manage Growing Cybersecurity Concerns

Richard Jaenicke, Mercury's Director of Strategic Marketing and Alliances, gave a presentation at the Embedded TechTrends conference in January 2018 entitled "*Trusted Computing: The Convergence of Trusted, Safe and Secure*". By the middle of 2018 after our initial report, Jaenicke had left his position at Mercury.<sup>1</sup>

Between Jaenicke's departure and the loss of its CISO and CIO, Mercury appears to have very few (if any) well-tenured executives or employees with deep knowledge of or experience in the cybersecurity space.



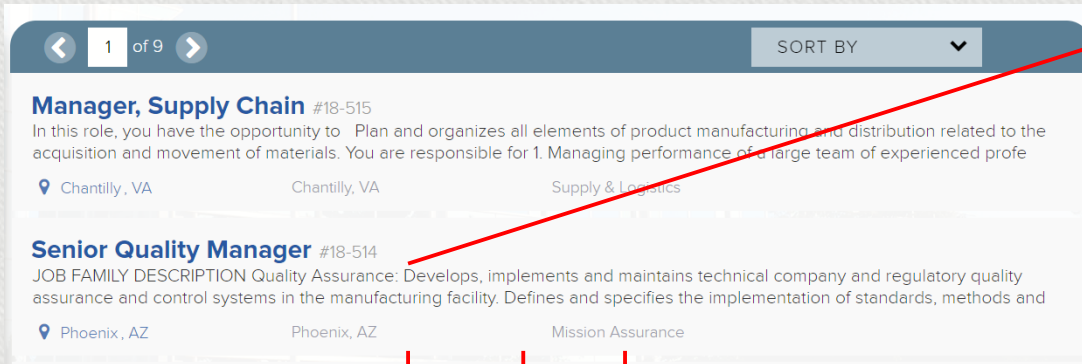
The screenshot shows a presentation slide for Mercury Systems. The slide features the Mercury Systems logo in the top right corner. The title is "Trusted Computing: The Convergence of Trusted, Safe, and Secure". Below the title, the speaker is identified as Richard Jaenicke, Director of Strategic Marketing and Alliances, with the email address Richard.Jaenicke@mrccy.com. At the bottom of the slide, there is a row of six circular icons representing different industries: a submarine, a truck, a rocket, a ship, an airplane, and a satellite. The slide is set against a background of a network diagram with white lines connecting various nodes.

Source: [Embedded Tech Trends](#) – Jan 2018

(1) Richard Jaenicke's LinkedIn [biography](#). This [link](#) suggests he left sometime after May 2018.

# Mercury Is Hiring In Exactly The Areas One Would Expect...

Just last week, on October 11, Mercury opened positions for “Supply Chain Manager” and “Senior Quality Manager”.  
**What more evidence do you need that Mercury has deficiencies in this area and costs are rising?**  
**We find the job description for “Senior Quality Manager” particularly interesting in light of the Supermicro news...**



**Manager, Supply Chain** #18-515  
 In this role, you have the opportunity to Plan and organizes all elements of product manufacturing and distribution related to the acquisition and movement of materials. You are responsible for 1. Managing performance of a large team of experienced prof...

Chantilly, VA | Chantilly, VA | Supply & Logistics

**Senior Quality Manager** #18-514  
 JOB FAMILY DESCRIPTION Quality Assurance: Develops, implements and maintains technical company and regulatory quality assurance and control systems in the manufacturing facility. Defines and specifies the implementation of standards, methods and

Phoenix, AZ | Phoenix, AZ | Mission Assurance

Source: Mercury [Careers Website](#)

**This job is in Mercury’s rugged secure microelectronics division, which manufactures products containing Supermicro components**

**POSITION SUMMARY**

Bring your expertise in Quality Management to a robustly growing organization to ensure that we bolster our reputation for high quality work in service of end applications where failure is not an option. Microelectronics Secure Solutions is a business unit of Mercury Systems that delivers dense, rugged, secure, trusted microelectronics packaging to the defense industry. We go to market with High Density Secure Memories, secure and rugged SSDs and custom MCM solutions.

- Lead a team of quality professionals that will
  - Work with Purchasing staff to establish quality requirements from external suppliers and monitor their performance
  - Ensure compliance with customer, national and international quality standards
  - Act as liaison with customers' auditors ensuring the execution of corrective action and compliance with customers' specifications
  - Audit manufacturing procedures and processes, both internal and at suppliers
  - Timely review and disposition of customer quality flow downs on purchase orders

**Management now concerned about the quality of suppliers following the Supermicro fiasco?**

**Looking for people to ensure compliance with new cybersecurity-related IT manufacturing regulations?**

**Need people to manage product recalls, etc. in response to discoveries of cybersecurity threats like the Supermicro issue?**

**Making a greater effort to ensure cybersecurity standards are met among manufacturers of componentry?**

# Newly Disclosed “Government Relations” Board Committee

Looking carefully, we find in Mercury’s proxy statement filed in September 2018 mention of a newly-created Government Relations Committee – created in 2017, but not disclosed until late 2018.

The #1 committee priority stresses “*identifying and evaluating global security...issues, trends, opportunities, and challenges that could impact our business activities and performance*”.

Does the creation of this committee suggest challenges with government relationships or a lack of important government relationships in the cybersecurity space?

## ***Government Relations Committee***

The Government Relations Committee, consisting of three or more members as appointed by the Board, was created in 2017 to assist the Board with the following functions:

#1  
Objective  
“Security”

- identifying and evaluating global security, political, budgetary, regulatory and other issues, trends, opportunities, and challenges that could impact our business activities and performance;
- making recommendations to continue to raise our visibility in the marketplace and awareness of our commercial business model, as well as our products and capabilities; and
- making recommendations concerning our government relations activities, including our interactions with local, state and federal government on matters of impact to our business with the aim of enhancing our customer base.

In carrying out its duties and responsibilities, the Government Relations Committee has the authority to meet with and make inquiries of our employees as well as obtain advice and assistance from external advisors.

Source: Mercury Systems 2018 [Proxy Statement](#); compare verses [previous proxy statement](#)

# We Hope Mercury Made Accurate Reps/Warranties To Its Bankers...

On October 1, 2018 Mercury filed Amendment No. 3 with the SEC stating that it had expanded its credit facility to \$750m, extended the maturity to Sept 28, 2023 and reduced its interest rate. It currently has \$240m outstanding on the facility.

As part of this amendment, Mercury made certain reps and warranties including that “No Material Adverse Effect” had taken place since closing. Does removing Supermicro as a key technology partner qualify?

### 3. Representations and Warranties.

On and as of the Amendment No. 3 Effective Date, the Borrower hereby represents and warrants to the Administrative Agent and each New Revolving Credit Lender, after giving effect to the amendments set forth in this Amendment, that:

(a) The representations and warranties of the Borrower and each other Credit Party contained in Article 6 of the Amended Credit Agreement or any other Credit Document are true and correct in all material respects (except that any representation and warranty that is qualified as to “materiality” or “Material Adverse Effect” or similar language is true and correct (after giving effect to any qualification therein) in all respects) on and as of the date hereof, except to the extent that such representations and warranties specifically refer to an earlier date, in which case they shall be true and correct in all material respects (except that any representation and warranty that is qualified as to “materiality” or “Material Adverse Effect” or similar language shall be true and correct (after giving effect to any qualification therein) in all respects) as of such earlier date; and

(b) No Default or Event of Default exists.

#### Section 6.05. *Financial Statements.*

The Annual Financial Statements fairly present in all material respects the financial condition of the Borrower and its Subsidiaries, as of the date thereof and their results of operations for the period covered thereby in accordance with GAAP consistently applied throughout the period covered thereby, except as otherwise expressly noted therein.

Section 6.06. *No Material Adverse Effect.* Since the Closing Date, there has been no event or circumstance, either individually or in the aggregate, that has had or could reasonably be expected to have a Material Adverse Effect.

“**Material Adverse Effect**” means (a) a material adverse change in, or a material adverse effect upon, the operations, business, assets, properties, liabilities (actual or contingent) or financial condition of the Borrower and its Restricted Subsidiaries, taken as a whole; (b) a material adverse effect of the ability of the Credit Parties, as a whole, to perform their payment obligations under the Credit Documents; or (c) a material adverse effect upon the rights and remedies available to the Lenders or the Administrative Agent under any Credit Document.



## *Evidence of Financial Strain In Mercury's Financial Disclosures*



# Mercury's Credit Agreement Points To Financial Misrepresentation

Mercury has claimed that cash flow will be fine in FY19, yet it just increased the size of its credit facility from \$400m to \$750m. In the process, Mercury divulged more evidence of financial misrepresentation. Mercury stated that it Amended its Credit Agreement on Dec 21, 2017. However, it never made mention of this Amendment, which would have been a material event requiring an 8-K financial disclosure. Mercury also should have mentioned that its A/R factoring began on Dec 2017, but this was not disclosed until Feb 2, 2018 when the 10-Q was filed. Mercury's FY18 operating cash flow is inflated by \$18.8m (43% of total).

## AMENDMENT NO. 3

This AMENDMENT NO. 3 dated as of September 28, 2018 (this "Amendment"), is entered into among MERCURY SYSTEMS, INC., a Massachusetts corporation (the "Borrower"), certain subsidiaries of the Borrower, as Guarantors, the Lenders party hereto (collectively, the "Lenders" and individually, a "Lender"), and BANK OF AMERICA, N.A., in its capacity as administrative agent for the Lenders (in such capacity, the "Administrative Agent"), and amends the Credit Agreement dated as of May 2, 2016 (as amended, supplemented or otherwise modified from time to time prior to the date hereof, including pursuant to Amendment No. 1, dated as of June 27, 2017, and Amendment No. 2, dated as of December 21, 2017, the "Existing Credit Agreement") entered into among the Borrower, the Guarantors party thereto, the Lenders from time to time party thereto and the other parties thereto. Capitalized terms used herein and not otherwise defined herein shall have the meanings ascribed to them in the Amended Credit Agreement (as defined below).

Source: Mercury [8-K](#) filed 10/1/18

## Potentially Deceptive MD&A on Cash Flow – Have To Dig Deeper For A Clearer Picture

*"During fiscal 2018, we generated \$43.3 million in cash from operating activities compared to \$59.1 million in cash generated from operating activities in fiscal 2017. The decrease was primarily a result of higher cash uses for income tax payables, accounts payables, accounts receivables and inventory. The decrease was partially offset by higher comparable net income, additional depreciation and amortization expense and deferred revenues and customer advances."*

Source: FY 18 [10-K](#), p. 41

On Oct 1, 2018  
Mercury  
Discloses a  
2<sup>nd</sup> Amendment  
on 12/21/17

Yet Just  
2 Months  
Earlier On  
Aug 16, 2018  
Mercury  
Still Claimed  
The Last  
Amendment  
Was June 2017

### Revolving Credit Facilities

In June 2017, we amended the Revolver, increasing and extending it into a \$400.0 million, 5-year revolving credit line expiring in June 2022. In connection with the amendment, we repaid the remaining outstanding principal and interest on our term loan using cash on hand. To facilitate the acquisition of Themis, we drew \$195.0 million from the Revolver, with the higher amount reflecting an estimated adjustment for working capital. See Note L in the accompanying consolidated financial statements for further discussion of the Revolver.

### Accounts Receivable Factoring

On December 21, 2017, we executed a Master Receivables Purchase Agreement (the "Purchase Agreement") with Bank of America, N.A. (the "Bank") for the sale of certain eligible accounts receivable balances of the Company, up to a maximum of \$30.0 million. Factoring under the Purchase Agreement is treated as a true sale of accounts receivable by us. We have continued involvement in servicing accounts receivable under the Purchase Agreement, but have no significant retained interests related to the factored accounts receivable.

Proceeds from amounts factored are recorded as an increase to cash and a reduction to accounts receivable outstanding in the consolidated balance sheets. Cash flows attributable to factoring are reflected as cash flows from operating activities in our consolidated statements of cash flows. Factoring fees are included as selling, general, and administrative expenses in the Company's consolidated statements of operations and comprehensive income.

We factored accounts receivable and incurred factoring fees of \$18.8 million and \$0.1 million, respectively, during the second quarter of fiscal 2018. We did not factor any accounts receivable or incur any factoring fees during the second half of fiscal 2018.

Source: Mercury [10-K](#) filed 8/16/18

# A Closer Look At Mercury's Inventory And Backlog

Mercury's current inventory and planned inventory purchase obligations relative to its next 12 months of backlog continue to remain elevated above historical norms.

\$ in mm	Q4'16	Q1'17	Q2'17	Q3'17	Q4'17	Q1'18	Q2'18	Q3'18	Q4'18
	6/30/2016	9/30/2016	12/31/2016	3/31/2017	6/30/2017	9/30/2017	12/31/2017	3/31/18	6/30/18
Inventory Purchase Obligations <sup>1</sup>	\$32.2	\$39.3	\$41.6	\$36.7	\$59.2	\$54.0	\$50.7	\$57.1	\$50.3
Current Inventory	\$58.3	\$58.4	\$70.1	\$72.1	\$81.1	\$93.3	\$105.9	\$117.1	\$108.6
<b>Total Obligations and Inventory</b>	<b>\$90.5</b>	<b>\$97.8</b>	<b>\$111.7</b>	<b>\$108.8</b>	<b>\$140.2</b>	<b>\$147.3</b>	<b>\$156.6</b>	<b>\$174.2</b>	<b>\$158.9</b>
Next 12 Months Backlog <sup>2</sup>	\$239.2	\$247.3	\$279.0	\$270.0	\$290.8	\$281.7	\$310.4	\$321.0	\$328.5
<b>Obligations &amp; Inventory / NTM Backlog</b>	<b>37.8%</b>	<b>39.5%</b>	<b>40.0%</b>	<b>40.3%</b>	<b>48.2%</b>	<b>52.3%</b>	<b>50.4%</b>	<b>54.2%</b>	<b>48.3%</b>

Period Chief Acct'g Officer Resign, Mechanism to Report Accounting Concerns and Insider Sales Begin

Larger Gross Margin Miss, First Sales and Earnings Miss


Record High

Still Elevated Above Historical Average

- 1) Reported under "Commitments, Contractual Obligations, and Contingencies". Per Mercury, "Purchase obligations represent open non-cancelable purchase commitments for certain inventory components and services used in normal operations."
- 2) Reported as the backlog to be shipped in the next twelve months.

# Next Twelve Month Backlog As A Percentage Of Total Backlog At A Multi-Year Low

Visibility and quality of Mercury's backlog appears to be deteriorating.  
It just reported a multiyear low of backlog expected to be shipped over the next twelve months.

FY Ended June \$ in mm	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018
<b>Ending Order Backlog</b>	\$104.6	\$140.3	\$174.1	\$208.0	\$287.7	\$357.0	\$447.1
<b>Backlog To Be Shipped Next 12 Months (NTM)</b>	\$91.9	\$113.2	\$144.0	\$166.5	\$239.2	\$290.8	\$328.5
<b>NTM Backlog % of Total Backlog</b>	87.6%	80.7%	82.7%	80.0%	83.1%	81.0%	 73.5%

Source: Mercury financial filings

# Artificial Boost To Earnings By Under-Accruing For Warranty Reserves?

The evidence suggests that Mercury has been aware of growing cybersecurity issues for some time, yet it has not been accruing for warranties in proportion to its growing revenues – especially from the Themis acquisition. In fact, warranty accruals as a % of revenues has declined every single year, even though Mercury states that “product sales generally include a 12 month standard hardware warranty”.

By under accruing for warranties, could Mercury be materially overstating its future EPS?

	Fiscal 2018	Fiscal 2017	Fiscal 2016
Beginning balance at July 1,	\$ 1,691	\$ 1,523	\$ 1,974
Warranty assumed from Themis	117	—	—
Warranty assumed from CES	—	176	—
Warranty assumed from Delta	—	30	—
Warranty assumed from Carve-Out Business	—	—	114
Accruals for warranties issued during the period	1,318	1,328	1,976
Settlements made during the period	(1,790)	(1,366)	(2,541)
Ending balance at June 30,	\$ 1,336	\$ 1,691	\$ 1,523

Source: Mercury 10-K

**Accrual Declines Every Year**

\$ in thousands	FY 2018	FY 2017	FY 2016
Accrual	\$1,318	\$1,328	\$1,976
Total Sales	\$493,184	\$408,588	\$270,154
Accrual % of Sales	0.27% ↓	0.33% ↓	0.73%

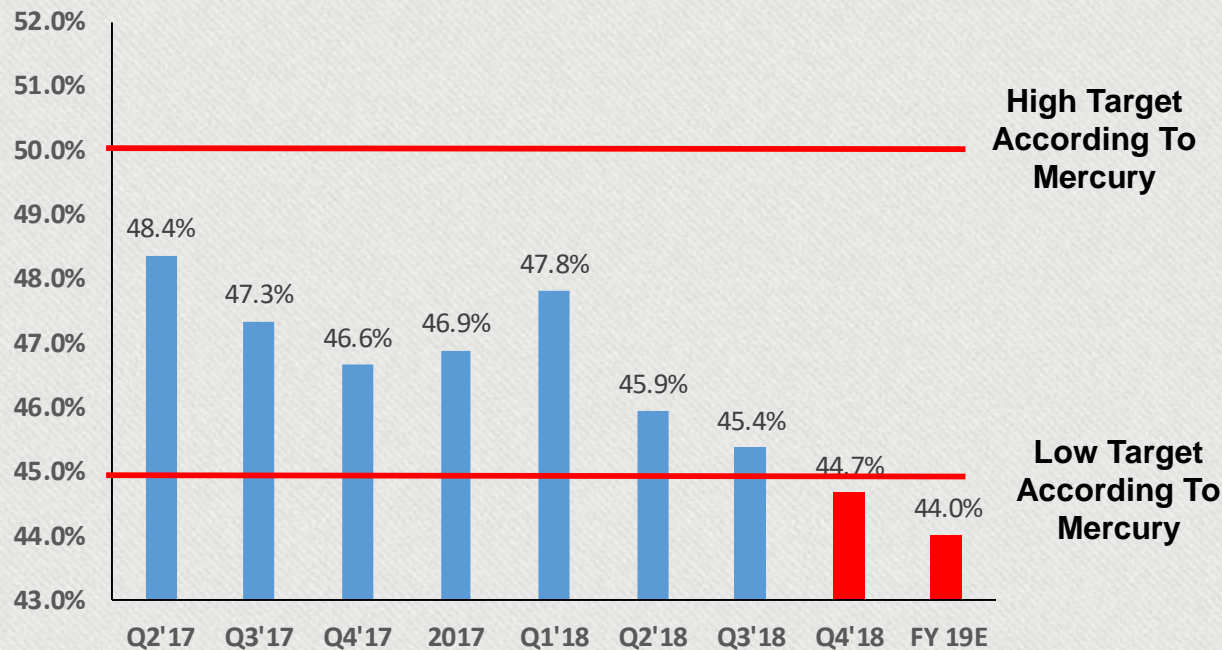
# Gross Margins Continue To Decline While Mercury Disappoints Long-Term Goals....

Mercury is now spinning excuses for gross margin contraction as related to acquisitions...while not quantifying any added costs related to the loss of its small business designation, DFARS compliance requirements, or potential recalls and/or new product costs related to replacing Supermicro as a technology partner.

**CEO Aslett on [Q4'18 Earnings Call](#):**

- “Gross margin was affected by product mix, including an increase in customer-funded R&D and early-stage programs. The inclusion of Themis, which has lower gross margins as well as an inventory step-up associated with the Themis purchase accounting.”
- “Germane will be dilutive to our gross margin and adjusted EBITDA margin in FY 2019, but accretive to fiscal 2019 adjusted EPS”

**Mercury Gross Margin Falling Below Lower Target Band**



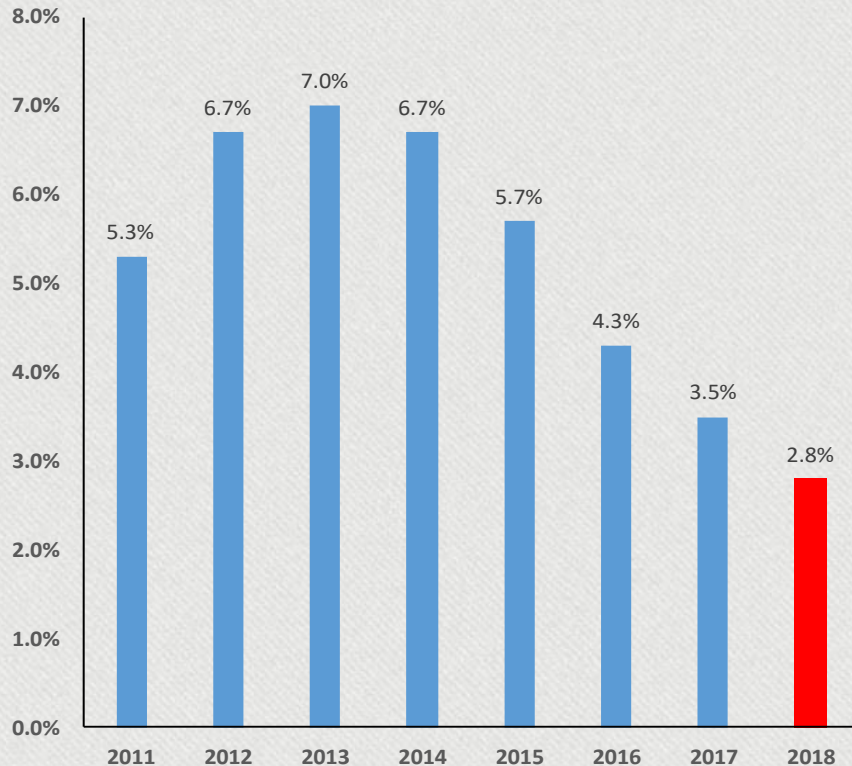


*Insiders Keep Selling, So Should You:  
50% Downside Risk Remains*

# Insider Selling Remains Rampant

Insiders continue to be net sellers of Mercury shares despite having been given the chance to prove Spruce Point wrong: rather than demonstrate confidence in the business by committing more personal capital at depressed prices, they have continued to sell out. Total insider ownership is now at a record low of 2.8%, which any long-term owner of the stock should find troubling.

## Total Insider Beneficial Ownership Hits New Lows Post Our Critical Short Report



Source: Mercury proxy statements

## CEO Aslett Stock Sales Continue Post Our Report....

Date	Shares	Price	Proceeds
9/27/2018	1,755	\$55.09	\$96,683
9/26/2018	2,945	\$54.84	\$161,504
9/21/2018	300	\$52.96	\$15,888
9/20/2018	10,000	\$52.28	\$522,800
9/19/2018	20,000	\$55.41	\$1,108,200
<b>Total:</b>	<b>98,184</b>	<b>\$54.43</b>	<b>\$1,905,075</b>

## COO Thibaud Stock Sales Continue Post Our Report....

Date	Shares	Price	Proceeds
9/17/2018	3,500	\$55.97	\$195,895
9/04/2018	3,500	\$54.60	\$191,100
8/15/2018	3,500	\$49.43	\$173,005
8/1/2018	28,000	\$48.80	\$1,366,400
<b>Total:</b>	<b>38,500</b>	<b>\$50.04</b>	<b>\$1,926,400</b>

Source: Bloomberg

Note: Only one token insider buy from the CFO of 3,100 shares

# Poor Risk/Reward When “Consensus” View Is That Everything Is Fine....

Analysts have not critically evaluated the impact of Mercury’s relationship with Supermicro and the increased exposure stemming from its recent acquisitions of Themis and Germane Systems. In short, analysts blissfully endorse the acquisitions and pencil both a new \$100m revenue stream and future margin expansion without pushing back on management’s assumptions.

Broker	Canaccord	SunTrust	Baird	Drexel Hamilton	JP Morgan	Jefferies	Average Price Target	Implied Upside
Price Target	\$64	\$61	\$59	\$58	\$52	\$44	\$56	+9%

**JPMorgan  
July 2018**

**“Overweight”  
\$52 Price  
Target**

- *“Mercury is building a C4I rugged server business. Mercury highlighted how its acquisition of Germane benefits from its FY18 acquisition of Themis, which the company views as a platform to build upon. The two entities have complementary rugged server portfolios and cover much of the C4I market with an expected ~\$100 mn in revenue. Near-term, the Germane acquisition is dilutive to company-wide profitability but Mercury should achieve cost synergies after integrating the units and believes the combined entity will reach the midpoint of MRCY’s adjusted EBITDA margin target in 2020”*

**Canaccord  
Oct 2018**

**“Buy”  
\$64 Price Target**

- *“Acquisition focus strengthens competitive and market position Mercury has completed a series of acquisitions since 2011 that have transformed the company’s focus and strategy. Specifically, the acquisitions have both positioned the company for greater growth in its target markets, and more recently positioned the company to drive margin improvement. For example, the Themis Computer and Germane Systems acquisitions created a \$100M C2I business focused on rugged servers.”*
- *“Investor reaction to Mercury’s acquisitions has been positive as we believe the company has done an impressive job of successfully integrating companies into its operations over the course of years and leveraging the results.”*

**Jefferies  
July 2018**

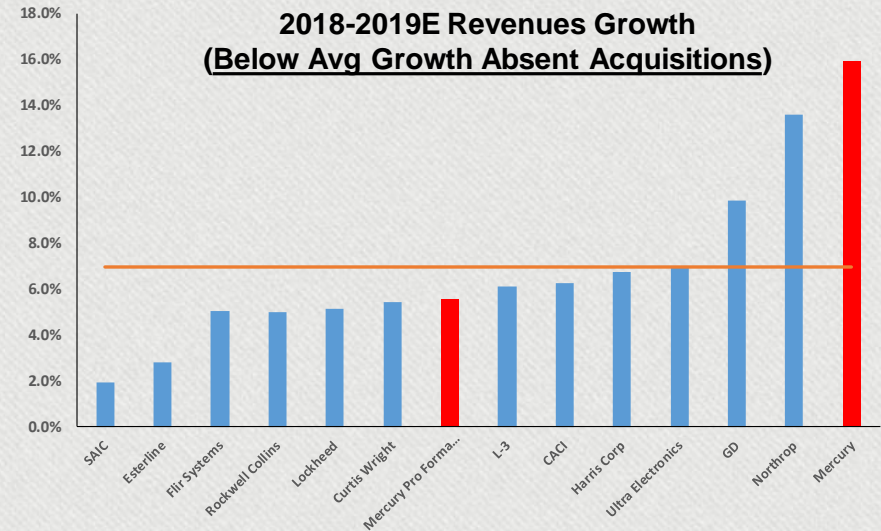
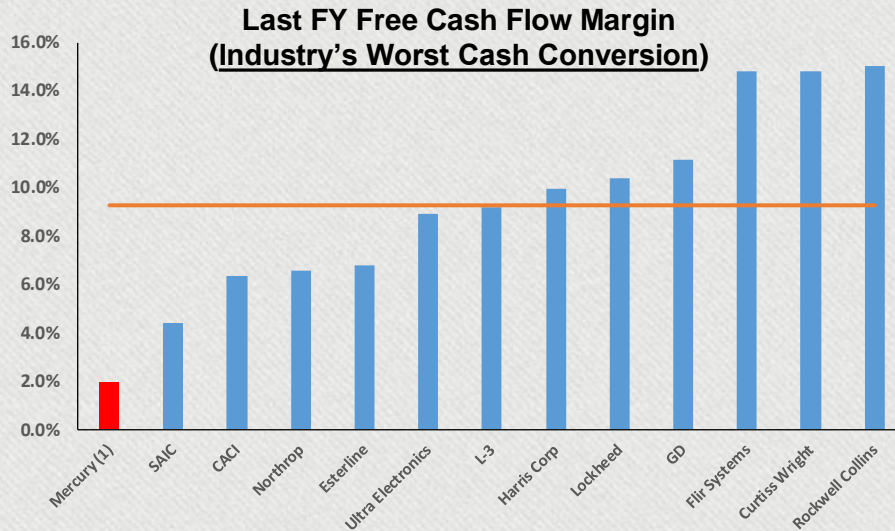
**“Hold”  
\$44 Price Target**

- *“Germane Systems is a provider of rugged services and storage systems for command and control (C2I) applications. The transaction is \$0.05 accretive on our estimates but dilutive to group margins. Themis increased MRCY’s capability in common processing systems with a platform to pick up share in the C2I arena. The \$5MM of run rate synergies are from cost synergies and potential product transformation”*
- *“On a market-relative basis, MRCY trades at a ~40% premium to S&P on FY2 PE, down from a 3-year average premium of 65%. MRCY trades at a 4.3% FY2 FCF yield vs peer average of 5.7%”*

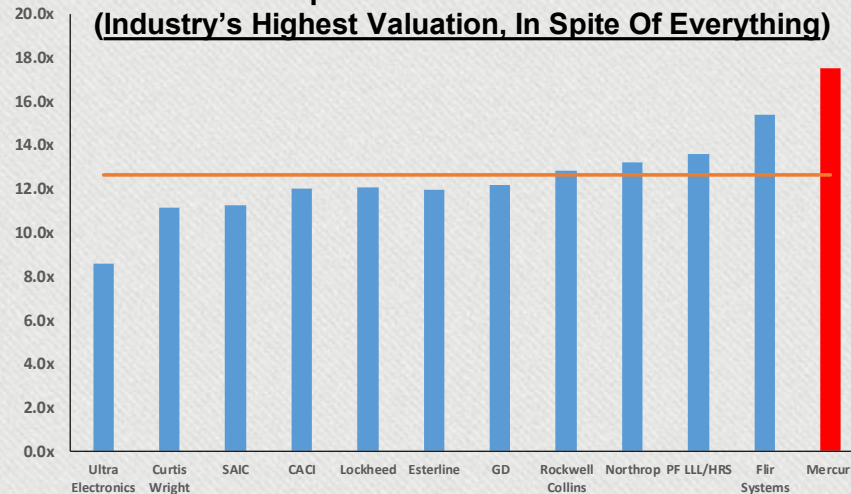


# Mercury Remains The Most Expensive, Weakest Cash Generator In Its Industry

Investors continue to ascribe an irrational valuation to Mercury despite its below average growth and poor cash conversion.



### Enterprise Value / 2019E EBITDA (Industry's Highest Valuation, In Spite Of Everything)



Source: Company financials, Bloomberg and Spruce Pt. estimates  
 Note: Esterline to be acquired by Transdigm  
 1) Pro forma Mercury organic revenue growth takes consensus calendar year revenues and excludes \$100m of revenues from Themis and Germane. Free cash flow is adjusted for \$18.8m of factored receivables

# Spruce Point Estimates 50%-60% Downside Risk

We believe the Street is structurally misunderstanding the magnitude of the cybersecurity-related costs that Mercury will face going forward, as well as the delays in revenue contract award opportunities it will face in its high-growth “command, control, communications, computers, and intelligence” (C4I) segment – expected to be a \$100m business. Mercury does not even have a CISO at present, and only recently replaced its departed CIO.

\$ in millions, except per share amounts

Valuation	Best Case Price	Worst Case Price	Note
<p><b>Sales Multiple</b></p> <p>CY Street 2019E Sales</p> <p><u>Spruce Point Adjusted</u></p> <p>Enterprise Value</p> <p>Plus: Cash</p> <p>Less: Debt</p> <p><u>Dil. Shares</u></p> <p>Price Target</p> <p>% Downside</p>	<p>2.0x</p> <p>\$645.8</p> <p><u>\$635.8</u></p> <p>\$1,272</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$23.12/sh</b></p> <p>-55%</p>	<p>2.0x</p> <p>\$645.8</p> <p><u>\$630.8</u></p> <p>\$1,262</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$22.91/sh</b></p> <p>-56%</p>	<ul style="list-style-type: none"> <li>Mercury has suggested that its Themis / Germane business will add \$100m of revenues, but with its recent removal of its tech partnership with Supermicro – which it says supports “short lead times” – there is bound to be slippage to revenue expectations</li> <li>Furthermore, we expect the added burden of having to comply with new DFARS regulations to delay contract awards. Mercury must now certify its cybersecurity requirements.</li> <li>Our worst case assumes Mercury achieves 85% of run rate revenues, and base case assumes 90% of its C4I rugged server expectations</li> <li>Mercury trades at 4x sales vs. the industry at 2x. Given serious security overhangs, Mercury’s multiple should compress to the industry average.</li> </ul>
<p><b>Multiple of EBITDA</b></p> <p>CY Street 2019E EBITDA</p> <p><u>Spruce Point Adjusted</u></p> <p>Enterprise Value</p> <p>Plus: Cash</p> <p>Less: Debt</p> <p><u>Dil. Shares</u></p> <p>Price Target</p> <p>% Downside</p>	<p>12.5x</p> <p>\$146</p> <p><u>\$114</u></p> <p>\$1,425</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$26.35/sh</b></p> <p>-49%</p>	<p>12.5x</p> <p>\$146</p> <p><u>\$83</u></p> <p>\$1,037</p> <p>\$66.5</p> <p>(\$240)</p> <p>47.5</p> <p><b>\$18.20/sh</b></p> <p>-65%</p>	<ul style="list-style-type: none"> <li>We layer in additional long-term costs for the new DFARS cybersecurity compliance requirements</li> <li>Our industry expert with 30yrs+ experience working with major primes in contracting and compliance believes that companies like Mercury should be prepared to absorb up to 10% of revenues to deal with new regulatory requirements. We model this as a worst case outcome, and 5% as base case</li> <li>In the event that Mercury acquires a cybersecurity company rather than develop needed cybersecurity capabilities in-house, it would effectively be capitalizing the cost with no revenue benefit, and with incremental interest expense cost</li> <li>Peer average multiple of 12.5x</li> </ul>
<p><b>Multiple of EPS</b></p> <p>CY Street 2019E EPS</p> <p><u>Spruce Point Adj EPS</u></p> <p>Price Target</p> <p>% Downside</p>	<p>18.0x</p> <p>\$1.84</p> <p><u>\$1.07</u></p> <p><b>\$19.26</b></p> <p>-63%</p>	<p>18.0x</p> <p>\$1.84</p> <p><u>\$0.54</u></p> <p><b>\$9.79</b></p> <p>-81%</p>	<ul style="list-style-type: none"> <li>Depreciation and Amortization of \$41.5m</li> <li>Tax rate of 20%</li> <li>Interest expense of \$9.6m (\$240m @ 3.9%)</li> <li>Peer average multiple of 18x</li> </ul>



*Appendix: Further Instances Of  
Mercury Wiping Supermicro  
References From Its Website*

# Mercury Purged Its Website Of Supermicro References Almost Entirely

That Mercury cleansed its website of Supermicro references almost entirely such a short time after the hacking story broke is deeply concerning – both because it suggests that management is genuinely concerned about the security implications of the hack, and because management went out of its way to sweep its connection to Supermicro under the rug as quietly as possible.

If the product risk is real – as management’s actions suggest – it should have been disclosed, not swept away.

## Themis Rugged Enterprise Servers Product Page: Before Hacking Story Breaks

## Themis Rugged Enterprise Servers Product Page: After Hacking Story Breaks

Home → Products → RES Servers

### Rugged Enterprise Servers (RES)

#### Resilient Cutting Edge Technology

Featuring leading-edge components that include Intel CPUs, NVIDIA Tesla GPU accelerators, and SuperMicro motherboards, Mercury RES servers are SWaP-optimized to deliver industry-leading performance in a smaller footprint. Rugged Enterprise Servers keep mission-critical applications available with enhanced reliability features and superior resilience to shock, vibration, and temperature extremes.

#### Configuration Versatility

RES servers provide maximum configuration flexibility through a range of size and depth, and front and rear I/O models. Featuring expansion slots, extensive high-speed I/O, and multiple storage options, our rugged servers provide users with configuration versatility to meet current and future system requirements. RES servers can be mounted in standard commercial racks or mobile rugged transit cases.



RES Server Dual Redundant Power

Standard Rackmount

#### Performance & Reliability for Rugged Environments

High Density

High Performance

Mini Servers

Resource Management

TMS' RES rack mountable servers are part of Mercury's Enterprise Series of advanced processing solutions that ensure superior performance and enhanced reliability in the most demanding environments. Combining leading-edge components that include Intel processors and SuperMicro motherboards, RES servers feature expansion slots, extensive high-speed front or rear I/O, storage, and enhanced reliability options to provide users with configuration versatility and system expansion to meet current and future system requirements.

→ RES-XR5 Standard Rack Mount Servers

Home → Products → RES Servers

### Rugged Enterprise Servers (RES)

#### Resilient Cutting Edge Technology

Featuring leading-edge components that include Intel CPUs and NVIDIA Tesla GPU accelerators, Mercury RES servers are SWaP-optimized to deliver industry-leading performance in a smaller footprint. Rugged Enterprise Servers keep mission-critical applications available with enhanced reliability features and superior resilience to shock, vibration, and temperature extremes.

#### Configuration Versatility

RES servers provide maximum configuration flexibility through a range of size and depth, and front and rear I/O models. Featuring expansion slots, extensive high-speed I/O, and multiple storage options, our rugged servers provide users with configuration versatility to meet current and future system requirements. RES servers can be mounted in standard commercial racks or mobile rugged transit cases.



RES Server Dual Redundant Power

Standard Rackmount

#### Performance & Reliability for Rugged Environments

High Density

High Performance

Mini Servers

Resource Management

TMS' RES rack mountable servers are part of Mercury's Enterprise Series of advanced processing solutions that ensure superior performance and enhanced reliability in the most demanding environments. Combining leading-edge components that include Intel processors, RES servers feature expansion slots, extensive high-speed front or rear I/O, storage, and enhanced reliability options to provide users with configuration versatility and system expansion to meet current and future system requirements.

→ RES-XR5 Standard Rack Mount Servers

# Mercury Purged Its Website Of Supermicro References Almost Entirely

## Themis RES-XR4 Rack Mountable Servers Product Page: Before Hacking Story Breaks

## Themis RES-XR4 Rack Mountable Servers Product Page: After Hacking Story Breaks

Home → Products → Legacy Solutions → RES-XR4 Rack Mountable Servers

### RES-XR4 Rack Mountable Servers

*Industry-Leading Performance, Enhanced Reliability and Superior Resilience to Shock, Vibration, and Temperature Extremes*

RES-XR4 rack mountable servers use Intel Xeon E5 2600 V2 processors with up to twelve cores to provide high reliability and performance to keep mission-critical applications available in the most demanding environments. Click on any of the links to go to the server product page.

RES rack mountable servers ensure superior performance and enhanced reliability in the most demanding environments. Combining leading-edge components that include Intel processors and SuperMicro motherboards, RES servers feature expansion slots, extensive high-speed front or rear I/O, storage, and enhanced reliability options to provide users with configuration versatility and system expansion to meet current and future system requirements. RES systems incorporate enhanced reliability features that include dual-redundant, hot swappable AC and DC power supply options. RES servers are an attractive solution for programs where SWaP are essential considerations. RES servers can be mounted in standard commercial racks or mobile, rugged transit cases.

Home → Products → Legacy Solutions → RES-XR4 Rack Mountable Servers

### RES-XR4 Rack Mountable Servers

*Industry-Leading Performance, Enhanced Reliability and Superior Resilience to Shock, Vibration, and Temperature Extremes*

RES-XR4 rack mountable servers use Intel Xeon E5 2600 V2 processors with up to twelve cores to provide high reliability and performance to keep mission-critical applications available in the most demanding environments. Click on any of the links to go to the server product page.

RES rack mountable servers ensure superior performance and enhanced reliability in the most demanding environments. Combining leading-edge components that include Intel processors, RES servers feature expansion slots, extensive high-speed front or rear I/O, storage, and enhanced reliability options to provide users with configuration versatility and system expansion to meet current and future system requirements. RES systems incorporate enhanced reliability features that include dual-redundant, hot swappable AC and DC power supply options. RES servers are an attractive solution for programs where SWaP are essential considerations. RES servers can be mounted in standard commercial racks or mobile, rugged transit cases.

Source: Themis Computer Products Page, RES-XR4 Rack Mountable Servers – [cached version](#) (8/21/2018) (archived [here](#))

Source: Themis Computer Products Page, RES-XR4 Rack Mountable Servers ([link](#), archived [here](#))

**Note that this is a legacy product. Therefore, the website alteration cannot be attributed to a genuine product spec change. This is simply blatant obfuscation.**

# Mercury Purged Its Website Of Supermicro References Almost Entirely

## Themis RES-XR4-1U Rack Mountable Servers Product Page: Before Hacking Story Breaks

Home → Products → Legacy Solutions → RES-XR4 Rack Mounta... → RES-XR4-1U Rack...

### RES-XR4-1U Rack Mountable Server (Dual Socket, 17 or 20 Inch Depths)

*Industry-Leading Performance, Enhanced Reliability and Superior Resilience to Shock, Vibration, and Temperature Extremes*

Featuring up to two E5-2400 or E5-2600 V2 Series Intel® Xeon® processors with up to **twelve cores**, a **Supermicro motherboard**, and 512 GB DDR3 ECC memory, the Themis RES-XR4-1U server provides industry-leading performance, enhanced reliability features, and superior resilience to shock, vibration, and temperature extremes. Designed for military, industrial, or rugged commercial use, the RES-XR4-1U server keep mission-critical applications available in demanding environments where Size, Weight, and Power (SWAP) is an important consideration.

The Themis RES-XR4-1U rack mountable server is a dual socket, 17 or 20 inch depth unit. The RES-XR4-1U server provides users with configuration versatility and system expansion to meet current and future system requirements. Themis RES-XR4-1U rack mounted servers can be mounted in standard commercial racks or mobile rugged transit cases.

Source: Themis Computer Products Page, RES-XR4-1U Rack Mountable Servers – [cached version](#) (9/2/2018) (archived [here](#))

## Themis RES-XR4-1U Rack Mountable Servers Product Page: After Hacking Story Breaks

Home → Products → Legacy Solutions → RES-XR4 Rack Mounta... → RES-XR4-1U Rack...

### RES-XR4-1U Rack Mountable Server (Dual Socket, 17 or 20 Inch Depths)

*Industry-Leading Performance, Enhanced Reliability and Superior Resilience to Shock, Vibration, and Temperature Extremes*

Featuring up to two E5-2400 or E5-2600 V2 Series Intel® Xeon® processors with up to **twelve cores** and 512 GB DDR3 ECC memory, the Themis RES-XR4-1U server provides industry-leading performance, enhanced reliability features, and superior resilience to shock, vibration, and temperature extremes. Designed for military, industrial, or rugged commercial use, the RES-XR4-1U server keep mission-critical applications available in demanding environments where Size, Weight, and Power (SWAP) is an important consideration.

The Themis RES-XR4-1U rack mountable server is a dual socket, 17 or 20 inch depth unit. The RES-XR4-1U server provides users with configuration versatility and system expansion to meet current and future system requirements. Themis RES-XR4-1U rack mounted servers can be mounted in standard commercial racks or mobile rugged transit cases.

Source: Themis Computer Products Page, RES-XR4-1U Rack Mountable Servers ([link](#), archived [here](#))

**Note that this is a legacy product. Therefore, the website alteration cannot be attributed to a genuine product spec change. This is simply blatant obfuscation.**

# Mercury Purged Its Website Of Supermicro References Almost Entirely

## Themis High Density Rackmount Servers Product Page: Before Hacking Story Breaks

## Themis High Density Rackmount Servers Product Page: After Hacking Story Breaks

### High Density Rackmount Servers



#### Compose Your Solution

Featuring 2U (four bay) or 3U (six bay) front I/O or rear I/O chassis options, Themis RES-HD 17" rack mountable servers provide maximum system configuration flexibility and functionality with over six types of "plug and pull" compute, storage, switch, expansion, and management modules.

Delivering superior performance with the latest Commercial Off-The-Shelf (COTS) components such as Intel® Xeon® Scalable processors and SuperMicro motherboards, Themis RES-HD servers reduce the overall costs associated with technology upgrades, logistics, lifecycle management, and ultimately the total cost of ownership.

Learn More:



Front I/O and Rear I/O Options:



### High Density Rackmount Servers



#### Compose Your Solution

Featuring 2U (four bay) or 3U (six bay) front I/O or rear I/O chassis options, Themis RES-HD 17" rack mountable servers provide maximum system configuration flexibility and functionality with over six types of "plug and pull" compute, storage, switch, expansion, and management modules.

Delivering superior performance with the latest Commercial Off-The-Shelf (COTS) components such as Intel® Xeon® Scalable processors, Themis RES-HD servers reduce the overall costs associated with technology upgrades, logistics, lifecycle management, and ultimately the total cost of ownership.

Learn More:



Front I/O and Rear I/O Options:



Source: Themis Computer Products Page, RES-XR4-1U Rack Mountable Servers – [cached version](#) (9/4/2018) (archived [here](#))

Source: Themis Computer Products Page, High Density Rackmount Servers ([link](#), archived [here](#))

# Mercury Purged Its Website Of Supermicro References Almost Entirely

## Themis High Density Systems Product Page: Before Hacking Story Breaks

## Themis High Density Systems Product Page: After Hacking Story Breaks

Home → [Solutions](#) → [Technologies & Expe...](#) → [High Density Systems](#)

Home → Solutions → Technologies & Expe... → High Density Systems

### High Density Systems

### High Density Systems

Function consolidation, virtualization, and big data analytics drive the requirement for more compute capability in a smaller footprint. The DoD requires feature-rich systems that interoperate in multiple applications and allow information sharing between applications. Demand is also driven by "Common Operating Environment" requirements, the use of [common components](#), and "right sizing" systems to deploy [solutions](#) in as many places as possible.

Function consolidation, virtualization, and big data analytics drive the requirement for more compute capability in a smaller footprint. The DoD requires feature-rich systems that interoperate in multiple applications and allow information sharing between applications. Demand is also driven by "Common Operating Environment" requirements, the use of [common components](#), and "right sizing" systems to deploy solutions in as many places as possible.

To support big data analytics, the DoD utilizes the Map/Reduce function initially developed by Google for search purposes and provided by Apache in Hadoop clusters. The U.S. Army currently utilizes Hadoop for mining sensor data in the DCGS-A program. The Army is constrained by size, weight, power consumption, and heat. Designed for virtualization, ISR, Big Data Analytics, radar processing, image processing, and large Hadoop cluster applications, [Themis HD](#) systems are part of Mercury's EnterpriseSeries of processing [solutions](#) which can be used in a multitude of applications that require high-compute density and low latency access to large-data storage. Suited for computing environments where server Size, Weight, and Power (SWaP) is important,

To support big data analytics, the DoD utilizes the Map/Reduce function initially developed by Google for search purposes and provided by Apache in Hadoop clusters. The U.S. Army currently utilizes Hadoop for mining sensor data in the DCGS-A program. The Army is constrained by size, weight, power consumption, and heat. Designed for virtualization, ISR, Big Data Analytics, radar processing, image processing, and large Hadoop cluster applications, Themis HD systems are part of Mercury's EnterpriseSeries of processing solutions which can be used in a multitude of applications that require high-compute density and low latency access to large-data storage. Suited for computing environments where server Size, Weight, and Power (SWaP) is important,

[Themis RES High Density \(HD\) servers](#):

[Themis RES High Density \(HD\) servers](#):

- Deliver high performance processing power
- Double compute density
- Enable a 50% rack space savings with per server weights as low as eleven pounds
- Reduce total system weight by nearly 50%

- Deliver high performance processing power
- Double compute density
- Enable a 50% rack space savings with per server weights as low as eleven pounds
- Reduce total system weight by nearly 50%



Designed with leading [commercial off-the-shelf \(COTS\)](#) components that include Intel® Xeon® Scalable processors and Supermicro motherboards, RES-HD servers provide maximum system configuration flexibility and system expansion options with processor, storage, high-speed switch, and system management module options.

Designed with leading [commercial off-the-shelf \(COTS\)](#) components that include Intel® Xeon® Scalable processors, RES-HD servers provide maximum system configuration flexibility and system expansion options with processor, storage, high-speed switch, and system management module options.

Source: Themis Computer Products Page, High Density Systems – [cached version](#) (8/10/2018) (archived [here](#))

Source: Themis Computer Products Page, High Density Systems ([link](#), archived [here](#))