The Complexity Crisis in Cybersecurity: **Simplify or Die!**

By: Steve Morgan, Editor-In-Chief Cybersecurity Ventures & Joseph Carson, CISSP, CSPO, CSP, Thycotic

As cyberattacks go mainstream, a simplified approach to cybersecurity will become mandatory.

INTRODUCTION

IT'S ENOUGH TO MAKE YOU WANNACRY OR SCREAM PETYA

In mid-May and again in late-June 2017, hackers exploited a vulnerability in Microsoft servers that was first discovered by the National Security Agency and then leaked online by a group of unknown hackers.(1) It allowed ransomware to spread across the world from server to server, encrypting as many files as it could, and holding more than 70,000 organizations victim in the process.

The so called "WannaCry" global cyberattack represented a milestone in cybercriminal activity hitting 200,000 computers in more than 150 countries over one weekend, and more recently "Petya" or "NotPetya" also causing havoc but this time without a "kill-switch" to help contain it. In effect, cyberattacks have gone mainstream, signifying that no one person or organization can consider themselves immune to the epidemic of malicious or criminal activity online. (2)

These latest incidents, and other high-profile breaches reported in the past few years, undercut the enormous effort and dollars spent to help keep information safe and secure.

Global spending on cybersecurity products and services is predicted to exceed $1 trillion cumulatively over the next 5 years - from 2017 to 2021 - according to a recent report from Cybersecurity Ventures.(3) More than ever, frustrated executives and boards of directors are seeking reassurances from cybersecurity professionals that they are getting a reasonable return on that investment.

THE COMPLEXITY CRISIS IN CYBERSECURITY

The "WannaCry" and "Petya" global cyberattacks leave no doubt about the critical state of our network systems' vulnerabilities.
It prompted the New York Times to run an opinion piece that asked, "The World Is Getting Hacked. Why Don't We Do More to Stop It?" (4)

Our cybersecurity defenses are no longer sustainable…they are too complex, too difficult to manage and as a result they are too costly—both in time and money. Thus, it's not surprising that breaches seem to be occurring at an accelerated rate and in greater numbers.

The truth is, many organizations today still do not have a clear strategy for protecting confidential or sensitive information.

Wind the clock back to 1999 when many companies where facing the famous Y2K bug, a challenge that had companies rushing to patch systems with an estimated fix cost of more than $400 billion.[5] At that time companies relied on complex mainframe computing systems that typically took months or even years to deploy. It wasn't unusual for software and IT management solutions to require highly skilled professionals to implement, using complicated configurations, and encyclopedic documentation. Getting professionals to use these systems also took months of training, with TCO running into millions of dollars.

One would expect that those days would be well behind us. Yet the state of cybersecurity today suggests we face similar challenges, with many companies unable to implement the protection and safeguards they need. While other technologies have steadily moved to the cloud, established virtualized solutions, and delivered software as services, cyber security has failed to keep pace with these trends.

As a result, far too many companies are installing and managing cybersecurity software "like it's 1999." Spending months to perform software upgrades or waiting for skilled professionals to become available is no longer a viable cybersecurity strategy. In the race to stop the rapidly morphing exploits of hackers and cyber criminals, complexity in cybersecurity solutions acts as a ball and chain, preventing us from ever catching up.

HISTORY SHOWS COMPLEXITY KILLS

The history of information technology is littered with examples where complexity literally killed major, multi-million-dollar projects aimed at improving performance.

For example, Gartner says that approximately 75 percent of all Enterprise Resource Planning projects fail, despite a massive effort to deliver better customer service and advanced IT systems.[6] An independent researcher speaking to decision makers about ERP projects noted that over half of businesses (48 percent) admit they find the range of solutions confusing. Half of them indicated a lack of industry standards or metrics makes it difficult to compare solutions and the flexibility of solutions are often unclear. Vendor providers confuse matters further with a lack of clarity about the costs (39 percent) and scheduling (35 percent) involved. That, in turn, leaves a third (33 percent) of businesses feeling unsure about the level of honest and transparent advice they are being offered.

A recent survey report by Thycotic researchers highlights a disturbing comparison with these ERP findings. The Security Measurement Index survey notes that nearly one-third of global companies and governments are making business decisions and purchasing cyber security technology blindly. These organizations simply don't possess sufficient data to know whether their investment decisions are actually making a difference in improving their overall cyber security posture. [7]

In a 2016 survey of 700 IT decision-makers from the US federal, state and education sectors, complexity of IT systems and technology was selected by the largest number of federal respondents — 42 percent — as their top difficulty in managing IT operations.[7] Asked about the biggest challenges facing their agency's IT operations, the largest number, 42 percent, selected cybersecurity, about two-thirds of federal respondents appear to lack the enterprise wide visibility and data automation needed for modern cybersecurity and IT operations.

Author and expert on national security policy, Dr. Stephen Bryen, summarized the situation in a recent blog, saying, "Today's systems are hugely complex and rapidly changing and adapting. Such complexity means that even with the best of intentions it is extremely difficult to cover all, or even most, of the potential vulnerabilities in operating systems, software, communications and networks. Virtually every modern system has been hacked successfully and repeatedly." [8]

The burden of complexity in cybersecurity is also aggravated by a growing shortage of skilled cybersecurity professionals required to manage ever more complex systems. A recent report from Cybersecurity Ventures predicts that there will be 3.5 million unfilled cybersecurity jobs by 2021. [9]

From obstruction to enablement: easy does it going forward Because of the complexity crisis in cybersecurity, many solutions set up an inevitable, never-ending conflict with productivity because of their demands on the time and efforts of IT department professionals. And in this constant battle between complex security vs. productivity, it's a sure bet that productivity will win by default.

Therefore, the cybersecurity industry must find more simplified solutions that are easier to deploy and manage. But given the growth in complexity, is that even possible?

A recent IDC Report called "Can Security Make IT More Productive?" describes an approach that will likely be driving an accelerated effort toward adopting simplified, yet effective, cybersecurity solutions.

"IDC data shows that over 80% of all innovations driven by business units were derailed by IT security concerns," according to the report. (10)

> **"This exacerbates executive management's negative perception. IDC believes that security is slowly undergoing a transformation from negative to positive and from obstruction to enablement. This enablement not only secures users, but can make IT more secure and productive by improving their user experience while automating tedious and error-prone processes."**

As cyberthreats become mainstream, organizations will have little choice but to accelerate the move to simpler solutions that remove complex management demands on IT staff while at the same time building in more secure, seamless processes.

SIMPLIFIED SOLUTIONS MEAN STREAMLINED, AUTOMATED TOOLS

The IDC report suggests the path from obstruction to enablement in cybersecurity is being forged according to four key principles.

STREAMLINED – Cybersecurity tools and solutions should support the business by allowing IT administrators to get their job done without slowing them down. This means that usability and efficiency are top of mind while still allowing for the appropriate security controls to be in place. Security tools don't need to be cumbersome – they can be efficient and secure if designed correctly.

SIMPLIFIED – Companies must look for and demand simpler solutions to problems. Solutions and tools should be designed with simplicity in mind. Every piece of complexity in security tools is a barrier to adoption, an invitation to circumvention, an obstacle to successful deployment, and a potential security risk.

AUTOMATED – Automated security functions may seem like a contradiction in terms for many security professionals, but with a shortage of skilled personnel, IT departments must rely on automation to keep pace with demand on limited resources.

ALWAYS SECURE – Access is a frequent weak link in daily operations as up to 80% of breaches involve some form of credential compromise. Cybersecurity must be woven into the fabric of the IT admin's workday, and become second nature, especially when it comes to accessing critical information involving privileged accounts and applications at the endpoint.

Refusing to accept complexity, and choosing more simplified cybersecurity solutions will help resolve a major issue with the shortage of skilled IT professionals. By choosing better ease of use, shorter install times, more efficient and effective upgrades and less documentation or training required, companies will be able to get and train a skilled workforce in much less time. Simplified solutions will ensure organizations have the human resources required to keep their business protected and secured.

THE SIMPLIFIED CYBERSECURITY IMPERATIVE

As the crisis in complexity for cybersecurity continues to escalate, the mandate to adopt more effective simplified solutions will only grow in importance. By implementing simplified, automated cybersecurity solutions that don't break the bank and actually contribute to the productivity of IT professionals, the cybersecurity industry could potentially save billions of dollars for its customers and an enormous amount of time and effort. Will complex cybersecurity be dead by 2020? If not exactly consigned to the graveyard, complexity will hopefully be greatly reduced or eliminated in the day-to-day lives of IT professionals across the globe.

EXAMPLE OF PASSWORD MANAGEMENT SIMPLIFIED

As a leading provider of Privileged Account Management (PAM) software solutions for on premise and cloud implementations, Thycotic represents a prime example of how to turn obstruction into enablement. As one of the easiest to use, implement, and customize PAM solutions, Thycotic products incorporate the key principles of a simplified solution.

Specializing in privileged credential security, Thycotic has developed its singular focus, attention, and resources on PAM solutions for more than 10 years. Thycotic Secret Server and Privilege Manager have been designed from the beginning as easy to use, simple to manage, and highly customizable solutions that deliver a comprehensive, end-to-end PAM security suite. That encompasses a wide range of functionality related to privileged credentials including: **Privileged Accounts, Privileged Access, Privileged Behavior, and Privileged Applications.**

Privilege Account Management Selection Criteria

CONVENTIONAL PAM SOLUTIONS **Legacy/heavy footprint**	**THYCOTIC PAM SOLUTIONS** **Designed for simplified operation**
Difficult to evaluate	Easy to try and compare
Multiple complex modules/extra costs	One comprehensive solution suite
Difficult to install	Easy to install in minutes
Takes weeks or months to get up to speed	Results from day one
Often requires expensive consulting	No consulting necessary
Needs multiple steps to manage properly	Manage in a few clicks
Staff must have extensive training to operate	No training required
1,000-page user manual	Manual only needed for occasional reference
Slow, tiered support response	Quick response by experts
Large expense upfront	Affordable, Cloud option

FLEXIBLE, SCALABLE FOR THE ENTERPRISE

Simplified does not mean PAM solutions are less robust or lack enterprise scalability. Thycotic PAM solutions such as Secret Server are easily customizable to fit a specific environment whether administrators rely on REST API or writing custom powershell scripts. Deployed at some of the largest global organizations around the world, Thycotic solutions are customers range from leading healthcare organizations to one of the largest energy corporations in the world. Thycotic PAM tools encompass the full Privilege Security spectrum of security, with High Availability and Geo-Replication capabilities to ensure that any global organization has an enterprise ready PAM security solution.

References

1 – *New York Times* https://www.nytimes.com/2017/04/15/us/shadow-brokers-nsa-hack-middle-east.html

2 – *New York Times* https://www.nytimes.com/2017/05/13/technology/hack-ransomware-scam-cyberattacks.html

3 – Cybersecurity Ventures http://www.cybersecurityventures.com/cybersecurity-market-report

4 – *New York Times* https://www.nytimes.com/2017/05/13/opinion/the-world-is-getting-hacked-why-dont-we-do-more-to-stop-it.html

5 – https://en.wikipedia.org/wiki/Year_2000_problem

6 – "Gartner: 75% of all ERP projects fail – But why? I Blog, May 9, 2017 https://www.linkedin.com/pulse/gartner-75-all-erp-projects-fail-why-blog-e-school-cloud

7 – "The 2017 State of Cybersecurity Metrics Annual Report" [Published July 27]

8 – "Why cybersecurity fails" http://www.bryensblog.com/why-cyber-security-fails/

9 – "Cybersecurity Has a Serious Talent Shortage" https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

10 – "Can Security Make IT More Productive?" IDC Spotlight on Technology, Dec. 2015 https://thycotic.com/why-thycotic/analysts-opinions/idc-report/

ABOUT THE AUTHORS

Steve Morgan, Editor-In-Chief Cybersecurity Ventures

Founder and CEO at Cybersecurity Ventures, and Editor-In-Chief of the Cybersecurity Market Report and the Cybersecurity 500 list of the world's hottest and most innovative cybersecurity companies. Steve writes the weekly Cybersecurity Business Report for IDG's CSO, and he is a contributing writer for several business, technology, and cybersecurity media properties.

Joseph Carson, CISSP, CSPO, CSP, Thycotic

Joseph Carson is a cybersecurity professional with more than 25 years' experience in enterprise security specializing in endpoint security, application security, and PAM. Joseph serves as Chief Secruity Scientist for Thycotic. He is a CISSP and an active member of the cybercommunity, speaking at cybersecurity conferences globally. He's a cybersecurity advisor to several governments, as well as critical infrastructure, financial and maritime industries.