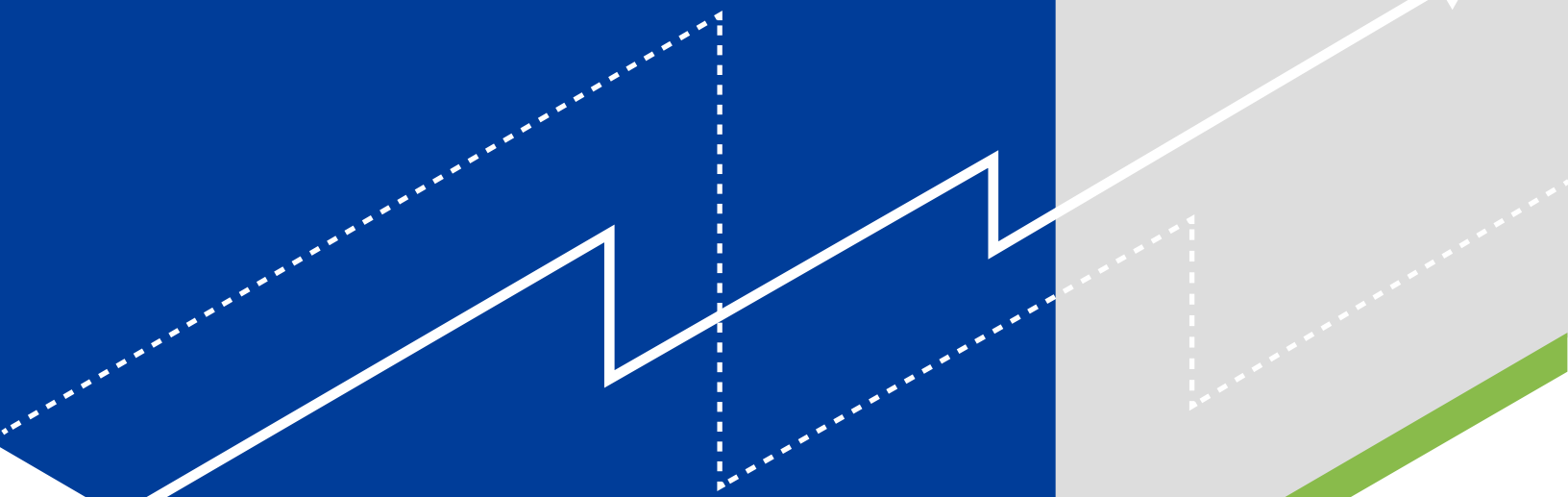
A Michael A. Echols
Thought Leadership Paper

2023

Better Business Security and Risk Management A Culture of Cybersecurity

Cybersecurity In A Box®

Mitigating Risk & Enhancing Cyber Performance In Critical Infrastructure Environments



MAX CYBERSECURITY LLC

Founder and CEO, Keynote Speaker, Author :
MICHAEL A. ECHOLS

Mike is the CEO of Max Cybersecurity LLC, located in Washington DC. He spent 17 years in critical infrastructure protection and cybersecurity leadership at the Department of Homeland Security. Mike led several White House national security risk initiatives prior to founding Max Cybersecurity LLC in 2017.

Mike is the author of a book *Secure Cyber LIfe, The Government is Not Coming To Save You*. He has also written four Forbes articles, been featured on PBS television's *Roadtrip Nation,* and led Critical Infrastructure Cyber Exercise for critical infrastructure entities.

National Cybersecurity Leadership

- **Operational Technology OT-CMF Founder**
  Cybersecurity Maturity Framework
- **APTA Facilitator**
  Control and Communications Working Group
- **Chair**
  Communication Sector Risk Assessment
- **Chair**
  National Small Business Cyber Assessment
- **Developed E.O. 13691**
  Information Sharing and Analysis Framework
- **Former CEO**
  International Association of Certified ISAO
- **Advisory Board**
  ICS-ISAC at Kennedy Space Center
- University of Maryland Smith School
  Advisory Board

Department of Homeland Security

- Designated Federal Official for Presidents NSTAC
- U.S. Representative NATO CCPC
- Director of Cyber Joint Program Management Office
- Director Government Industry Planning and Management Office

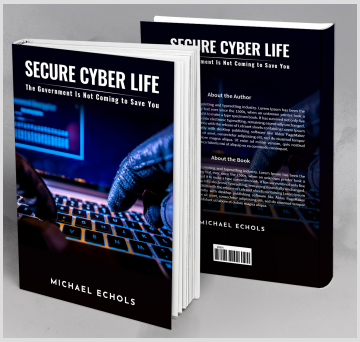
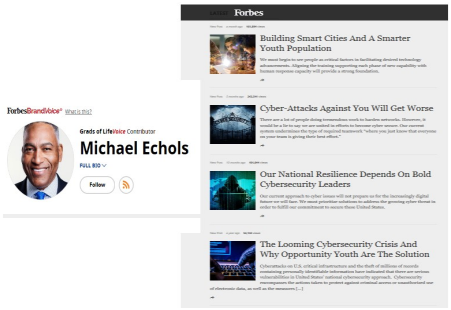


Table Of Contents

ABOUT MAX CYBERSECURITY LLC

Max Cybersecurity provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom risk management projects. Max Cybersecurity services connect you directly with analysts, cyber, thought-leaders and relevant government partners who apply expert insight to your specific business challenges. For more information, visit www.maxcybersecurity.com

MICHAEL ECHOLS info@maxcybersecurity.com



Executive Summary

While security has traditionally been reactive in nature, with its metrics focused on minimizing costs through breach avoidance, Max Cybersecurity provides the opportunity to define security more strategically with effective plans, proactive analysis and risk-based performance metrics.

Corporations, municipalities and business entities are finding it harder to remain cyber secure while staying compliant with emerging cybersecurity laws, and meeting the financial requirements to protect digital infrastructure. The costs associated with effective defense has escalated and the seemingly vast number of threat vectors expanded with each innovation.

In critical infrastructure service environments there are extended issues. Traditional Internet Technology (IT and Operational Technology (OT are bleeding together in a mess of technology. Some of these systems were never meant to be networked and their integration creates additional risks.

Most organizations define cyber-defense as a major cost. The value of implementing effective strategies prior to a cyber incident is often unclear. However, new statistics identify the average cost after a breach at $4.35 million, and as much as $200 million. Traditional methods of valuating the return on investment for security modernization, especially cybersecurity investment is also unclear. However, it is becoming clear that if existing best practices were implemented we could reduce the chance of a successful breach by 80%. This one fact is assisting to make the value of a defense-in-depth strategy that builds a culture of cybersecurity well worth the cost.

In today's competitive marketplace, cybersecurity is also becoming a crucial market differentiator. Companies increasingly realize that security is critical to: maintaining operations; securing intellectual property; assuring safety and security; and protecting their brand. More and more, customers want to do business with secure businesses — and since empowered customers can easily move their business elsewhere, security decision makers must understand and measure their program's effectiveness. Additionally, Board of Directors must be on the lookout for indications of failure that will create systematic risks and most harm the business. Lawmakers are looking closer at the role of the Board members to manage cyber risks.

Cybersecurity is most effectively delivered and executed as a team sport. That is, every member of the team has a role. This requires focus on the game and an understanding of vulnerabilities, threats and consequences to develop the most effective game plan. An entity must put an emphasis on helping the team members understand the challenge and rise to that challenge.

Organizational misalignment and technological complexity undermine even the best plans. The "Team" matters. Most cybersecurity failures for all businesses are typically iead to human fault or error. Lazy analysis, and at other times a failure to use best practice, are the culprit. When this occurs in an environment with a lack of visibility and poor observability across the enterprise, the potential for cascading consequences are high. Therefore, understanding and verifying, what is believed to be true about capabilities and capacity, people process and technology, is a key to resilience

Security has traditionally been reactive in nature, with its metrics focused on minimizing costs through breach avoidance. Max Cybersecurity provides the opportunity to define security more strategically with effective plans, proactive analysis and risk-based performance metrics. Though many security organizations seek to effectively implement systems to achieve this goal, many of the existing myopic approaches fail.

The truth is, the threat is ever-increasing. Therefore, solutions must be relevant and designed to balance security with business performance. Organizations of all kind must seek to build a culture of cybersecurity. This approach to security aligns people, process and technology. Most importantly, it tests assumptions and recognizes that the staff can be a force multiplier.

CYBERSECURITY: Is Risk Management

Business entities are finding it harder to remain compliant with emerging cybersecurity laws and the requirements to protect digital infrastructure. The costs associated with effective defense is escalating and the seemingly vast number of threat vectors are expanding. The desire for mobility and expansion of Internet of Things (IoT) connections has organizations continuously readjusting security baselines and defending against emerging threats. This shapes a new security-business paradigm:

- Business entities lack a common language surrounding cyber risk and need a comprehensive measurement that accounts for all potential sources of exposure beyond just the technical.
- There is a requirement for tools to continuously assess, diagnose and mitigate holistic business risk and enable cyber resilience through a shared culture of cybersecurity that permeates throughout organizations.

"The path to improving cybersecurity posture consists of three crucial steps. Maintaining cyber resilience entails continuously applying this cycle to instill a *Culture of Cybersecurity* that encourages a proactive organization-wide approach to sustaining what works and strategically addressing areas of deficiency."

Foundational Steps to Attain Cyber Resilience

The path to improving cyber security posture consists of three crucial steps. Maintaining cyber resilience entails continuously applying this cycle to instill a Risk Aware Lifestyle™ that encourages a proactive organization-wide approach to sustaining what works and strategically addressing areas of deficiency.

Collect

Paving the road to improved security posture starts with a multi-modality data capture process to create a data repository for subsequent analysis.

Compute

Maxxsure analyzes the collected data in combination with real-time data using its computational engine to compute your company's unique M-Score. The inputs into this model span remediations, training, policy changes, new controls, campaigns, continuous scans, patch updates, social media changes, non-cyber projects, and many more variables.

Communicate

Maxxsure offers custom dashboards, reports, and tools that promote conversations among the entire company leadership on how to operationalize programs that better manage risk.

What is M-Score?

The M-Score quantifies cybersecurity risk on a scale from 0 to 1,000, based on six pillars from which Maxxsure has derived a multitude of variables that comprise its proprietary scoring model.

› Communicating Security's Effectiveness to Key Audiences

› Security is evolving into a business discipline, but this isn't dawning on everyone in the security ranks equally. In the wake of an incident, C-level security decision makers are more likely than their staff to cite harm to company reputation and customer acquisition— meaning that C-level decision makers understand the value of effective security better than their direct reports.

› As the discipline matures, there will be better translation between executives and the organization: explaining up to the CEO what they are doing to secure the business' ability to generate more revenue, as well as explaining down to direct reports on why it's important to set security goals align security mission to business objectives.

› Companies can no longer simply share results of a successful audit to prove they have good security performance. CISOs understand that while their audits are important boxes to check, security outcomes are what really matter. Security leaders need to capture, track, and report on security metrics that truly measure security effectiveness, built on meaningful measurement that all stakeholders can understand.

Average Days to Discover and Mitigate Data Breach
206

Average Cost of a Data Breach
$4.35 Million

Most Expensive Country
United States

- Cyber attacks and security breaches are increasing in frequency and sophistication, with discovery after the fact, if at all.
- Targeting of organizations and individuals with malware and anonymization techniques, can evade current controls.
- Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defense and are rapidly becoming obsolete—Use encryption technology to avoid detection.
- Criminals are leveraging innovation and moving at a pace security vendors cannot possibly match.

The opinions of regulators, stakeholders customers and partners have begun to shape the cybersecurity decisions that companies make.

Cybersecurity in its essence is defending against a hundreds of adversary techniques. The level of defense is defined by adequate planning, preparing, system monitoring, analysis, execution and the ability to measure results. The main challenge to capable organizations is an ever-changing threat landscape, visibility and resource restrictions. Specifically, even when all the best protective systems are in place, the technical and management abilities of team members can define outcomes

You Can't Manage What You Can't Measure

Organizations must begin to manage their cyber systems through a knowledge focused len. Leaders are increasingly on the hook to answer questions like: **How does security align with and support overall business objectives? What goals should be set? And how does our defense stack up to known threats?** Cyber leaders need to understand the value of their system versus the metrics to understand cybersecurity performance. This approach also allows a Board of Director understanding of additional required spending.

- **Security metrics are becoming critical to planning budgets, but the maturity of managing security as a business is still low.** Security is evolving into a business discipline. There is increased scrutiny on spending, and formal metrics are now the key method to justify investments. In a recent Forrester study, 63% of security experts who responded advised that they measure key cybersecurity metrics. However, 63% is still low considering how important measurement is. And it's also important to note that 40% say they have warned decision makers of worst-case scenarios to rouse attention in order to justify investments — a far cry from a precise business case.

Consider Industrial Control System Environments - Chart Below

Items above the red line are likely missed by current approaches to cybersecurity.

Anti-virus, firewalls, VPNs, security update programs, intrusion detection and other standard approaches provide little protection against the current spectrum of attacks - Andrew Ginter

If this important fact is missed in risk assessment, an organization is blind to the risk.

Organized Crime	IT Insider	ICS Insider	Hacktivist	Intelligence Agency	Military
Virus triggers shutdown	Drop malware	Remote shutdown	Embarrass Business	Sleeper malware	Erase hard drives
Ransomware	Vandalism – delete files	Remote mis-operation	Remote shutdown	Remote shutdown	Remote mis-operation
Rem targeted ransomware	Remote shutdown	Drop malware	Erase hard drives	Erase hard drives	Sleeper malware
Rem targeted misoperation	Remote misoperation	Physical Vandalism	Remote misoperation	Remote misoperation	Autonomous malware
Disable safeties	Disable safeties	Local misoperation	Disable safeties	Disable safeties	Compromised insider

› **Other common security metrics tell an incomplete story.**
Four of the top five security metrics used today are flawed in several ways. Metrics like the number of malware incidents blocked or number of data loss prevention incidents generated are not contextualized figures (i.e., a company may count that the firewall blocked 1 million intrusions, but it doesn't report how many they let in). Other metrics in the top five, like the percentage of intrusions blocked by firewalls or the percentage of phishing emails filtered, may provide greater context (by reporting as a percentage). But, they can also miss the mark in other troubling ways, including: 1) Only reporting on the limited scope of what existing instrumentation measures, leading to potential blind spots, and 2) Highlighting information based on queries that only reflect the analytical skills of the architect, leading to bias. Traditional metrics paint an incomplete picture and can leave companies blind to potential risk.

Four of the top five security metrics used today are flawed

› **The board sees metrics that don't fully measure security's effectiveness.**
The intended audience for security metrics further highlights the CISO's challenge to be an effective security translator within the organization. 63%of firms that measure the number of blocked malware incidents also report the metric up to the board. But because this metric provides no larger context and is subject to analytical bias, it is inappropriate for strategic board-level discussions. Metrics like this don't meaningfully communicate exposure or performance to executives, regulators, business partners, or customers. However, one encouraging point of comparison in a recent Forrester Study is that 63% of companies using cybersecurity ratings also report them up to the board, and since these ratings are more risk-focused, objective, and outcome-based, they are appropriate for board-level discussions.

Metrics like number of blocked malware offers no context suitable for Boards

ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge.

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of cyber-attacks. They're displayed in matrices that are arranged by attack stages, from initial system access to data theft or machine control.

MITRE ATT&CK framework, a behavioral-based threat model, to identify relevant defensive sensors and build, test, and refine behavioral-based analytic detection capabilities using adversary emulation. This methodology can be applied to enhance enterprise network security through defensive gap analysis, endpoint security product evaluations, building and tuning behavioral analytics for a particular environment, and performing validation of defenses against a common threat model using a red team emulating known adversary behavior.

So, how do we make this information actionable to gain the highest value from threat intelligence? An easy way to start using ATT&CK for threat intelligence is to look at a single adversary group you care about. Identifying some behaviors they've used helps you inform your defenders about how they can try to detect that group (such as APT19).

Example: *Let your defenders know about the specific Registry run key APT19 has used. However, APT19 might change that and use a different run key. If you look at the Detection advice for the technique, you see a recommendation is to monitor the Registry for new run keys that you don't expect to see in your environment.*

Detection

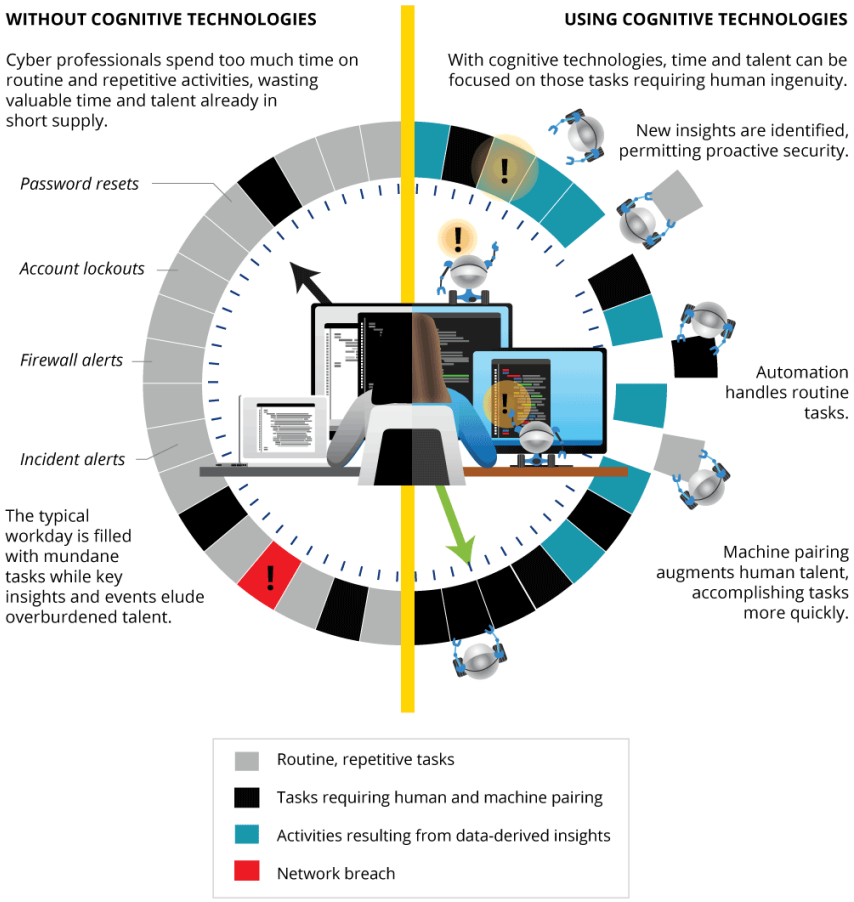
Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. [142] Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.

Cybersecurity Is A Team Sport

Hiring and retaining talent is critical to mature cyber systems. Every member of the team contributes to a capability defined by their combined knowledge and experience. Therefore, with the hiring of new talent and the continuous expansion of threats, it is difficult for any organization to maintain capabilities. It's even more difficult to assure each team member has awareness of all threats and best practices as defined by their technical and risk environment.

To keep up with the expanding threat landscape and the resources requirement (financial and human), organizations need a force multiplier system. They need a way to enable a higher knowledge base for individuals who sit on the cyber team. The goal is to make them all better. In this case, *better* is knowing policies, understanding the threat against specific vulnerabilities and being able to efficiently check for specific attack indicators. This will allow an organization to maintain a risk-reducing environment and response system that is based on best practices, but within the guidelines of the organization.

Figure 1. The cyber professionals' workload



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

What is the Most Effective Use for the Cyber Professional's Time?

How Can Artificial Intelligence Help?

Why Share Cyber Threat Information

Cyber threat information sharing is essential to thwarting successful hacks and minimizing consequences should a breach occur.

Cyber attacks have increased in frequency and sophistication, presenting significant challenges for organizations that must defend their data and systems. These threat actors range from individual, autonomous attackers to well-resourced groups operating in a coordinated manner as part of a criminal enterprise or on behalf of a nation-state.

Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, and expose or steal intellectual property and other sensitive information. Given the risks these threats present, it is increasingly important that organizations share cyber threat information and use it to improve their security posture.

Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. By exchanging cyber data within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber threat information from multiple sources, an organization can also enrich existing information and make it more actionable.

This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information through the reduction of ambiguity and errors. Additionally, sharing of cyber threat information allows organizations to better detect campaigns that target particular industry sectors, business entities, or institutions.

EFFECTIVE USE OF RESOURCES: BUILDING A CULTURE OF CYBERSECURITY INCREASES THE CYBERSECURITY RETURN OF INVESTMENT

So far, our discussion has focused on how prioritizing and scoring help companies 1) reduce risk 2) more effectively manage their cybersecurity approach measure performance, so that security leaders can report up and out on effectiveness. However, better use of existing human resources is like increasing the size of the security team while promoting excellence in practice. That excellence, may just reduce the overall costs of cybersecurity for an organization with more engaged employees.

Cybersecurity in its essence is defending against a few hundred adversary techniques. The level of defense is defined by adequate planning, preparing, system monitoring, analysis, execution and the ability to measure results. The main challenge to capable organizations is an ever-changing threat landscape, visibility and resource restrictions. Specifically, even when all the best protective systems are in place, the technical and management abilities of team members can define outcomes.

There's not a person alive who hasn't made mistakes. In fact, making mistakes is a core part of the human experience - it is how we grow and learn. Yet, in cybersecurity, human mistakes are far too often overlooked.

According to a study by IBM, human error is the main cause of 95% of cybersecurity breaches. In other words, if human error was somehow eliminated entirely, 19 out of 20 cyber breaches may not have taken place at all!

"When all the best protective systems are in place, the technical and management abilities of team members can define outcomes."

› **Mature companies will seek to reduce risks related to every process and technology in their enterprise.**

In 2020 alone, multiple cities and counties had their systems locked with demands from hackers for a ransom to have their data returned.

The implementation and development of a "culture of cybersecurity" might have mitigated the impact of these attacks.

An organization can get started by implementing the NIST Cybersecurity Framework.

The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) organizes basic cybersecurity activities at their highest level. These highest levels are known as functions:

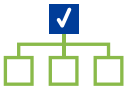
- Identify
- Protect
- Detect
- Respond
- Recovery

These functions help agencies manage cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and learning from previous activities.

Categories are subdivisions of a function. They group cybersecurity outcomes closely tied to programmatic needs and particular activities.

Key Recommendations

Performance measurement helps you analyze and articulate the effectiveness of your program within your organization. Most importantly, it assists to the overall value of your cybersecurity investment. Not all security metrics are made equally, and getting to the point where you can accurately measure and communicate security risk to your business is no easy task. By implementing programs to understand your cybersecurity approach versus the threat, and score risk an organization can takes control. The organization can then implement practices across the enterprise to create a culture of cybersecurity.



Seize the opportunity while senior executives focus on cybersecurity. Cybersecurity is now a board-level topic and one that senior business stakeholders believe contributes to the financial performance of their firm. Develop meaningful security metrics that highlight how an effective security program helps preserve and protect brand and reputation to avoid squandering the spotlight.

Build-in security to support the future growth of your digital enterprise brand by measuring security performance. For security leaders seeking to increase their credibility with senior business leaders and their firm's board of directors, there is no better way to improve confidence in cybersecurity than with a set of mature processes. The approach should show a steady growth in security culture that is consistent with increasing digitalization and, the convergence of IT and OT.

Leverage threat metrics to combat the data deluge and make better decisions for your business. When it comes to establishing meaningful metrics, security leaders are often their own worst enemy. The instinct to solve security problems with technology results in a complex technology ecosystem with a growing amount of disjointed data and no way to analyze it. Risk-based metrics help you understand where and how you need to prioritize investments in your security program. In addition to immediate decisions, they help you plan for future decisions, as well as view the results of prior decisions.

Keep a laser focus on customers, partners, and business cybersecurity performance to lower enterprise risk. Align your program metrics to your business metrics to understand how your business creates value for customers. Connect your metrics to the relevant customer-facing employees, data, applications, systems, and processes. Mature metrics connected to your business will make the effectiveness of your security program clear when you share your metrics with customers, partners, and other non-security colleagues.

MICHAEL A. ECHOLS
Contact me: mechols@maxcybersecurity.com