CYBERSECURITY IN THE '20'S: SOLVING THE GAPS

"Cybersecurity is the biggest risk facing business today"
– Warren Buffett

1. Executive Summary

Cybersecurity is a challenging and risk-laden field, one that many in senior management struggle to truly understand. A recent survey by Swiss Re showed that 85% of senior management regard cybersecurity as the greatest threat to earnings, yet 90% reported they had no insight into their own cybersecurity effectiveness.

This extreme level of imbalance persists at most organizations in nearly every industry. **How do we get to a better place, and properly protect the enterprise**? We examine new and emerging ways to analyze, prioritize, and address the gaps remaining today in areas of effectiveness and transparency.

Our conclusion focuses on the area of people – the capabilities of the cybersecurity professionals themselves – as the real difference-maker in this all-important battle between capabilities and ever-present threats.

2. Intro – Where Are We Now?

> *"You can dream, design and build the most wonderful place in the world, but it requires people to make the dream a reality"*
> — Walt Disney

At a basic level, real-world, economically measurable cybersecurity losses have expanded radically in the past two decades to become the largest business-related source of economic loss of all risk categories, and now surpass even Property & Casualty losses by roughly four times. The facts paint a very serious picture:

- Over $800bn in annual global losses to cybersecurity attacks – and growing by double digits year-on-year
- Radical expansion in ransomware, particularly large-scale, enterprise-level ransomware attacks
- A significant uptick in nation-state attacks, and in the proliferation of military-grade exploit kits out to the broader dark web attacker domains
- Regularity of shareholder litigation following most significant breaches
- Increased pressure from regulators around compliance requirements including timely public disclosure
- Over $180bn in annual cybersecurity spending globally, without a significant reduction in the rate of loss expansion

Many worthy analyses of the cybersecurity landscape are in circulation. Nearly all of these portray the rapidly expanding nature of the threats. Threats are advancing at least as fast as our most sophisticated protections, and their sophistication and scope of use is growing faster. At the same time, organizations are challenged with how to prioritize, and where to invest their cybersecurity budget.

Patch management, technology asset management, threat intelligence and risk management remain some of the top, most challenging areas for organizations to solve for in advancing cybersecurity protections. Yet none of these is more challenging than the talent gap. Nearly every public and private organization is finding a worsening situation in recruiting and retaining effective staff and specialists in fighting this all-important battle. We can throw technology at the problem by writing checks. Much more difficult is the sourcing of the right people and filling the key roles that are often the real difference-maker in our all-important defenses.

We examine these issues here, and how every organization can take steps to radically advance their cybersecurity protection by solving first and foremost for the talent gap. We end with a summary of key actions that any organization can begin taking now on a path to a more secure future.

3. Goals and Issues – Where Do We Need to Be?

"People are not your most important asset. The right people are."
— Jim Collins, Good to Great

Cybersecurity, in its present form, derived from information security, whose principles date to the Roman Empire. Military use of codes and ciphers to protect strategies and tactics have been used for thousands of years. Today, however, we have a vastly greater set of challenges, due to the very nature of society in the 21st century. Leading factors driving the complexity of today's cybersecurity challenges include:

- Pervasive use of, and dependency on technology across all global regions, demographic groups, and age categories
- Rapid expansion of new technologies, often focused on functionality as opposed to protection
- Widespread access to very sophisticated threat technology
- A robust and illegal market for stolen data, as well as a market for the purchase and distribution of thousands of malware and attack technology for sale to anyone
- Little or no prosecution possible in many global jurisdictions, resulting in zero consequences for attackers even after being identified
- Increasingly lucrative economic incentives for attackers, especially in ransomware, where ransom payoffs are expanding into the tens of millions, and cyber insurance providers are now regularly funding the payment of ransoms
- The institutionalization of attacker organizations, with 50, 75, or more workers operating openly out of office space in their home jurisdiction, where hiring dozens of PhDs, researchers, malware developers, and other professionals is very inexpensive
- The nurturing of independent, civilian attack organizations by host nation-states as both developers of weaponized cyber technology, as well as to launch attacks on geopolitical targets including private industry
- The continued uncertainty of cybersecurity insurance as a reliable method of cyber risk transfer, due to the deep set of exclusions written into most of these policies, coupled with the fact that relatively few policy provisions have been tested in court, resulting in extremely thin case law to rely on
- Most importantly, a complete unavailability of the properly trained professional specialist in the cybersecurity area, where retention is less than two years on average, and placement can easily average 18 months – even as many organizations seek to grow their staffing, and the total number of qualified professionals represent no more than 60% of the total active openings

Result: Where we need to be is characterized as starting with a complete, unvarnished acknowledgment of these conditions. Only then can we start devising, individually and collectively, our efforts to address the problem. The challenges are immense, and we need to fundamentally understand that this is one of the biggest problems of the 21st century and gear up for it accordingly.

4. Gap Analysis – What Do We Need to Solve For?

> *"If I am putting myself out there and taking some of these risks, then I want to do it properly."*
> – Daniel Ricciardo, Australian Formula 1 Driver

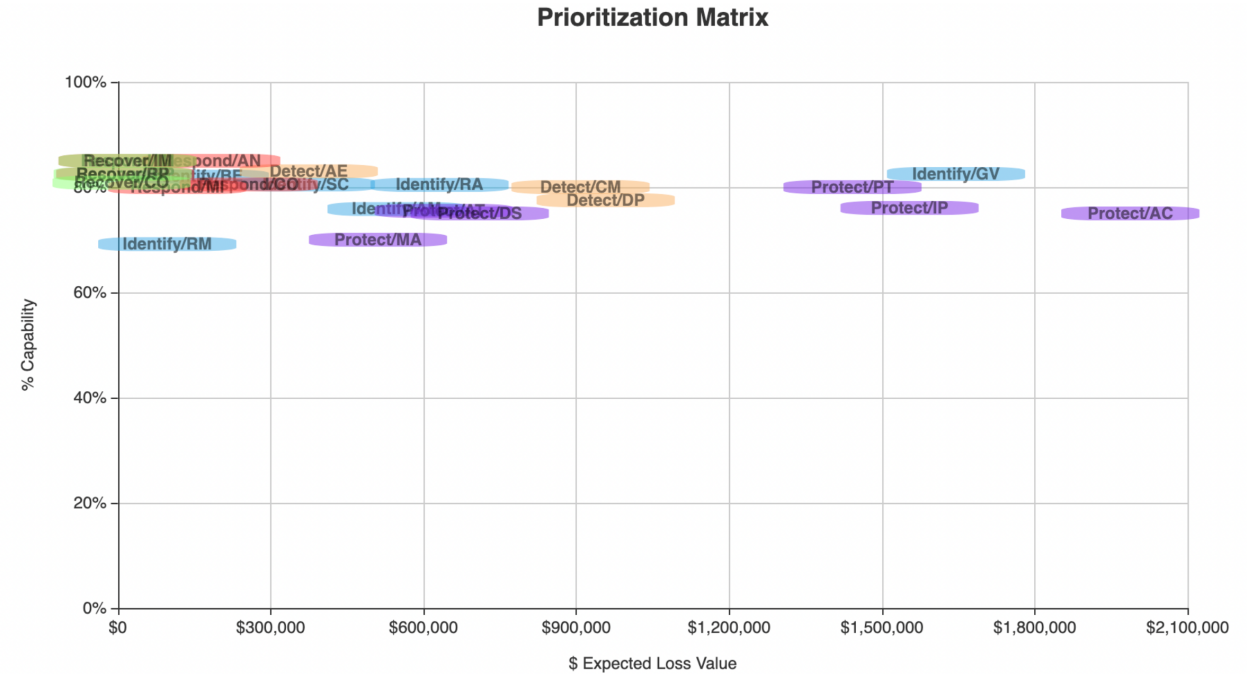
There are many places where these trends show themselves as issues and gaps to be solved. Often, organizations fail to separate between cause and effect. Just like a good medical doctor, we need to not confuse symptoms with root cause diseases. The stakes are too high in cybersecurity for us to make the mistake of simply treating surface symptoms and "hope" the patient will get better.

Consider the following:

GAP/CAUSE	SYMPTOM(S)
Cybersecurity organizational scope excludes IoT, Shadow IT, or other vulnerable domains	Inconsistent lines of authority for security, leading to inconsistent protections, as well as complete blind spots
Incomplete ability to identify threats	Surprise attacks where we have no defense
IT asset management inconsistencies unidentified/unmanaged and thus unprotected	Prospect of networks, servers, devices
Cloud instances with security configured inconsistently from "core" IT	Limited ability to create a normalized, single view of risks and vulnerabilities
Lagging ability to apply required patches	30/60/90-day period of open, exposed vulnerability across a wide range of systems

And, of course, the list goes on. Getting to the root cause of each surface condition identified is essential to devising and applying a correction that is predictable and lasting. Ideally, in most cybersecurity operations, there is a triage approach – one that seeks out the most impactful conditions, along with the ones that can be most easily fixed, and prioritizes them for resolution first, then working further down the list.
We can see how this may work, for example, across broad families of NIST (National

Institutes of Standards and Technology) cybersecurity families:



Here, we would be emphasizing the areas in the righthand side of the graph, since the risk exposure associated with these conditions is the greatest, while at the same time, the room for improvement – knowing that a series of these conditions are in a 40-50% capability range, means that they are much easier to advance than a condition that is at, say 80%.

Now – the typical set of actions following this level of analysis is, for most organizations, to propose and gain budget for new solutions to address these gaps. The good news is there are more highly effective technology solutions continuing to emerge to address these issues more effectively. But – are we missing something? What about staff to operate, monitor and direct these expanding and ever more complex solutions?

In most cybersecurity organizations today, the technology is expanded first, with new solutions being implemented at an ever-accelerating rate. Much of the hiring is then a following, not leading factor. But is this getting us the best result?

Most cybersecurity solutions take 60-90 days to implement, and even our most advanced AI-driven solutions that require a learning curve for the solution to adapt to our specific conditions are now fully implemented in four to six months. Yet the personnel to operate these sophisticated technologies – many requiring scarce specialists – take six to nine months or longer. Note that cybersecurity has the highest level of "shelfware" among all areas of IT – technologies that were approved, budgeted, and acquired – yet never implemented. The more effective tactic is to source the

people, then move on to the shorter-cycle implementation, assuring that we have the people to properly operate the new solutions to their utmost, by the time we go live.

National Cyber Group (herein referred to as NCG) professionals are the ones to trust to interpret the many and varied needs of each specific organization. And people bring the expertise to see where and how these technologies should be put to their best use. In every risk category, our people are the ones we need especially now, to properly interpret results, weed out false positives and false negatives, and guide us to the most effective ways to address the conditions and get at true root causes.

There are many places where these trends show themselves as issues and gaps to be solved. Often, organizations fail to separate between cause and effect.

Just like a good medical doctor, the best cybersecurity professionals focus on diagnosis first, and only then do they prescribe treatment. Think of your own visit to a trusted physician. Ideally, the discussion is about where it hurts, when it may have started, whether there's been any family history of similar conditions, and what you may have already tried to treat the conditions. Then, most physicians will say "let's run some tests" to get data. The goal is to get sufficient data to support a diagnosis – and to get the diagnosis right, because the alternative can have severe consequences – just like in cybersecurity.

Given the challenges in cybersecurity today, those practitioners who may lack professional grounding, including those who simply have basic certifications, may prematurely jump to a diagnostic conclusion – or worse yet an assumption. This pattern can result in life-threatening exposure for the enterprise, including a false assumption of proper security.

Overall, cybersecurity professionals have attained a very deep set of knowledge in technical solutions, integration, and how to deploy and operate these solutions. Yet, more is needed. What about the soft skills, and what about the professional standards, without which the profession cannot advance?

5. Action – How Do We Advance?

> *"If you think it's expensive to hire a professional to do the job, wait until you hire an amateur."*
> – Red Adair, Oil Firefighter

In the past, it was regarded by many as sufficient for the cybersecurity professional to attend a one-week bootcamp, gain a certification, and enter the career field. Feedback from professional and employers alike has shown that this legacy approach results in many specific training gaps, accompanied by the thinnest level of soft-skills preparation, insufficient for the increasingly complex challenges faced in today's environment.

In addressing these vital gaps in today's cybersecurity profession, National Cyber Group (NCG) has deployed several measures to elevate graduates and in turn, the standards for a professional practice that is so sorely needed.

These measures include:

- **The NCG Advisory Council:** A collection of top organizations from Aerospace, Financial Services, Healthcare, and other industries that guide the formulation of new subject material and core skills found to be differentiators in gaining truly effective cybersecurity in their own organizations
- **The NCG Code of Conduct:** Eleven basic principles that all NCG graduates ascribe to and use to guide their professional conduct
- **Trend Surveys:** Recurring feedback from our graduates, instructors, and other professionals in the field to further identify and calibrate to what's working best, as well as emerging trends in protective practices, shared with our overall community
- **Ecosystem:** Key relationships with CompTIA, CrowdStrike, Splunk, regulators and publishers, to incorporate their innovation and content into our community
- **Comprehensive Career Support:** Complete interaction and content for the cybersecurity career professional, through publications, free training, seminars, and emerging trend reports
- **Career-Long Partnership:** Beginning with secondary education, NCG provides early-stage, beginning-career, and advanced professional experiences at all levels to fully provide the career management tools and environment for the elite professional to launch, manage, and succeed throughout their careers
- **Standards:** By incorporating NIST, CISA, ISO and other standards as a reference point, NCG graduates can direct their efforts professionally to

support regulatory compliance, provide audit readiness, and litigation preparedness for their organizations in all they do

NCG continues to refine these profession-advancing features over time and to provide the most extensive ongoing educational and career-advancing opportunities to support our graduates in bringing the best to their organizations.

6. Summary – What Can I do Now?

> *"Hiring the Best is your most important task"*
> – Steve Jobs

When you look around at your own cybersecurity program or those of others, what do you see? Is the organization caught in the trap of *"We don't know cybersecurity, but we seem to have good people running our cyber program",* or is the organization getting truly transparent results from a professional corps that are truly at the top of their profession?

Ask your cybersecurity teams how they prioritize their efforts. Find out how well-integrated the many solutions and technologies in use really are.

- Is information consolidated to provide the all-important diagnosis of conditions?
- What additional measures may fill in gaps in the tests and data feeds being used to direct key cybersecurity efforts and initiatives?

Even fundamental metrics should be understood, and exposed by the cybersecurity team, to key leaders outside the technology organization – e.g. How many attacks are we getting? What percentage are successful? How do we compare to others in our industry? And what are our biggest risks, not just in our opinion but through data and analysis?

These are just the start of the key questions to ask. Regulators, industry groups and federal agencies have compiled many diagnostic tools, guides, rating systems and handbooks for the non-cybersecurity professional to gain an understanding of the key indicators and guideposts that can reveal the effectiveness and professionalism of the current cybersecurity practices of any organization.

Finally, realize that it is truly all about the people. Gaining the right people in the right roles is essential to get to truly effective cybersecurity. All organization have access to the same very advanced technologies and solutions. Yet some organizations have experienced far more severe losses than others.

About National Cyber Group:

Headquartered in the Washington D.C. metro area, National Cyber Group offers cyber security workforce development and talent solutions by combining the forces of Ameri- ca's most-known name in foundational IT certification training, Total Seminars, and the most hands-on cyber training program, CyberNow Labs, with new job placement and staffing solutions to attract, train and transmit thousands of career-seekers into entry-and-mid-level jobs as the nation's 'Elite Cybersecurity Corps.'

Learn more at **NationalCyber.com**

Resources

Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats – Forbes: https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=55f6f7486b61

Significant Cyber Incidents and Trends – Center for Strategic and International Studies: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure – Securities and Exchange Commission: https://www.sec.gov/rules/proposed/2022/33-11038.pdf

Perspectives on transforming cybersecurity – McKinsey & Company: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

Ransomware Surge – Fortune: https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/

Separating the Truths from the Myths in Cybersecurity – Ponemon Institute: https://www.ponemon.org/local/upload/file/BMC%20Consolidated%20Report%20Final.pdf

Shields Up – Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov/shields-up

Cyberthreat Defense Report 2022 – CyberEdge Group: https://cyber-edge.com/cdr/

Study: Hackers Attack Every 39 Seconds – University of Maryland: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

2021 Data Breach Investigations Report – Verizon: https://www.verizon.com/business/resources/reports/dbir/

Allianz Risk Barometer 2021 Rank 1: Cyber Incidents: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2022-cyber-incidents.html

How much does a data breach cost? – IBM: https://www.ibm.com/security/data-breach

Fact Sheet: Workforce Sprint – Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/21_0701_dhs-factsheet-workforce-sprint-july-2021.pdf