NISOS

How to Adapt: Managing Intelligence Needs During Economic Downturn

March 2023

Today's Topics

- Needs and priorities of finance during recession-impacted budgeting
- The evolution of managed services into managed intelligence
- Tools and expertise needed to run an advanced intel program
- Hiring advice for how to bridge talent and expertise gaps - aka The War for Talent
- Baselining intel expectations regarding people, processes and technology

Finance’s Needs and Priorities

- Flexibility
  - Be able to scale up quickly
  - Broaden capabilities cost-effectively
- Visibility
  - Understand true spend
  - Forecast business performance
- Accountability and responsibility
  - Get value/ROI on investments
  - Hold stakeholders accountable to results

Surviving the Downturn

Businesses of all sizes must make pragmatic decisions to survive, requiring a careful balance of economic considerations, growth plans, security needs, and workforce management.

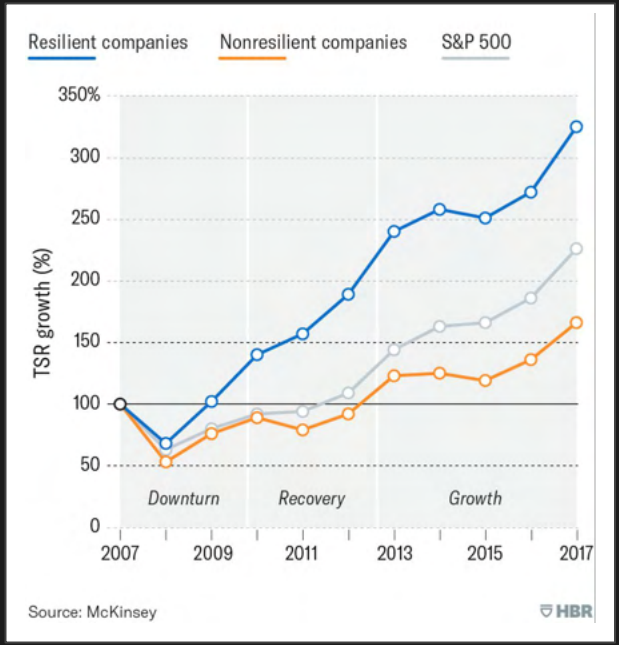
Course of Action	Approach	Questions to Consider
Maintain Status Quo	Many businesses will opt to stay the course, trusting that their current strategic roadmap will be viable despite difficulties.	■ What, if any, new obstacles has the recession created that may risk your roadmap? ■ What elements of your business operations are critical to maintaining continuity? ■ What risk/threats should you be most concerned about?
Invest & Acquire	A few businesses will be well positioned to take advantage of the shaky foundation of acquisition targets and seize the opportunity to buy up market share at a discount.	■ How has the recession impacted your chosen investment/M&A target? ■ Who is targeting your potential partner, and how? ■ How will a relationship with this third-party impact your risk profile?
Cut Costs	It's not easy to determine where to cut costs, especially when headcount reductions are in play. Cost-cutting strategies should focus on finding efficiencies in your teams' operations and ensuring continuity.	■ What tasks take up most of your team's time? ■ How can you ensure your team isn't wasting time on the wrong threats? ■ How can you ensure you don't miss threats because of budget reduction?

Criticality of Cost Controls

- Survival, resilience, and growth
  - McKinsey

2009

- Resilient organizations reduced their debt by more than $1 for every $1 of total capital on their balance sheet. Non-resilient companies added more than $3 of debt.

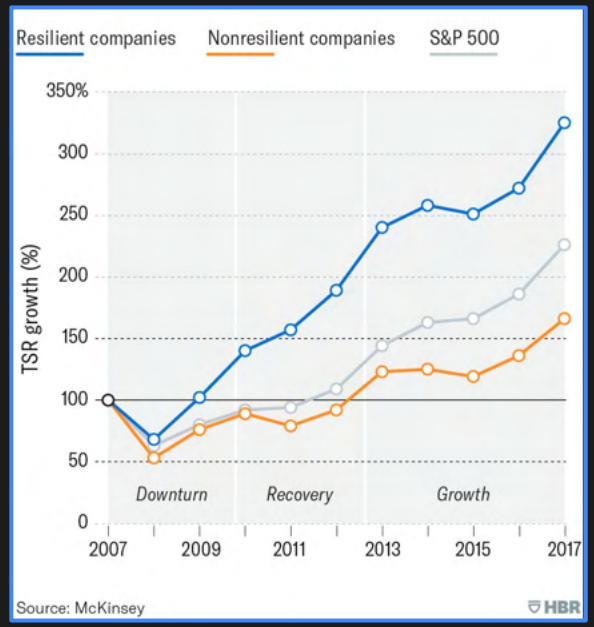


Cost Controls Were Critical

According to McKinsey & Company, cost controls were not just key to survival; they propelled resilient organizations' growth out of the recession faster than their less disciplined peers.

At its lowest point in 2009, organizations that would weather the recession and accelerate subsequent growth had increased their EBITDA by 10%, while industry peers had lost nearly 15%.

Put another way, resilient organizations reduced their debt by more than $1 for every $1 of total capital on their balance sheet. Non-resilient companies added more than $3 of debt.



The Great Recession (2008-2010)

The rate of economic decline accelerated quickly in the Fall of 2008:

- U.S. gross domestic product fell by 4.3%, the biggest drop since WWII
- Unemployment rate more than doubled, from less than 5% to 10%

Organizations of all sizes (and across all industries) had to make tough decisions to:

- Cut costs
- Trim marketing and research efforts
- Introduce layoffs and hiring freezes

"If your neighbor gets laid off,

it's a recession.

If you get laid off,

it's a depression."

Harry Truman

The 2010s: A Time of Technology-Driven Change

2010: 40 min	2022: 2 hours 20 min	2015: 30%	2022: 60%	2010: 4 devices	2022: 16 devices
Time Spent on Social Media Per Day		**Share of Corporate Data Stored in the Cloud**		**Average Number of Internet Connected Devices in the Household**	

- Rapid technological advancement as businesses and consumers became increasingly connected.
- Major breaches, constant cyber attacks, and advanced cyber weapons drove awareness of cybersecurity issues into the boardroom.
- Ransomware | Phishing | BEC | DOXXING | Malware

"The 2010s "...were the decade in which the last of our comfortable illusions of a free (libre), stable, and peaceful cyberspace were shattered…"

JD Work, Cyber Conflict and Security - Marine Corps University

Breaches that Broke Through to the Board

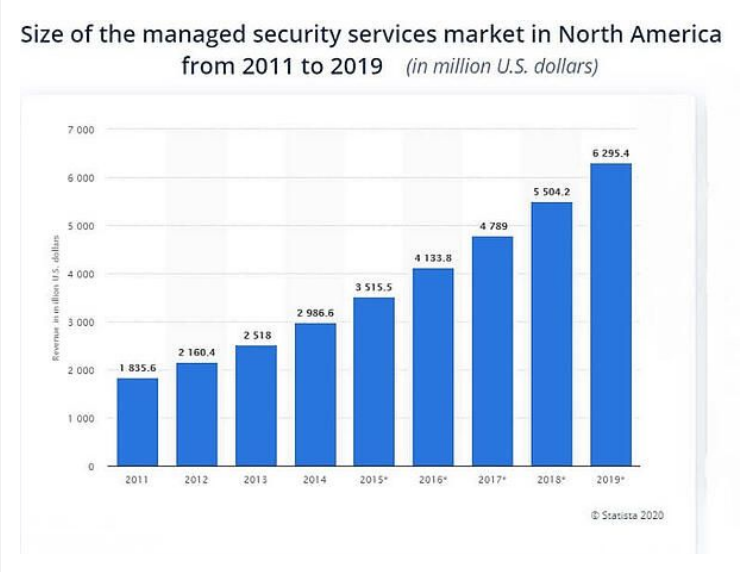
Before the 2010s, cybersecurity responsibilities were almost exclusively the concern of the IT team. Short of a catastrophe, it rarely got a second thought from executive leadership, let alone the board of directors. That's because, before 2010, cyber-attacks were typically limited in scope and minor in impact. The 2010s changed all that. **Now, cybersecurity is top of mind for the C-suite and is a common topic of discussion with the board, with 30% of security leaders briefing the board weekly.**

Stuxnet 2010	**Sony PlayStation 2011**	**Target 2013**
Sony Pictures 2014	**Yahoo 2016**	**WannaCry 2017**
	Petya & Not Petya 2017	

Managed Service Providers Become Trusted Security Partners

Common Security Tools Deployed and Managed by an MSSP:

1. Security Information Event Management (SIEM) Platform
2. Endpoint Protection Software
3. Cloud Security Tools
4. Email Security
5. Intrusion Prevention Systems (IPS)
6. Identity Access Management (IAM)
7. Privileged Access Management (PAM)
8. Data Loss Prevention (DLP)
9. Vulnerability Scanning



Today, 35% of security leaders fear they are wasting money on threats that aren't important. 40% report their teams are reaching the point of burnout as a result.

Vanson Bourne - State of Threat Intelligence 2022

Do-it-Yourself Intelligence is Difficult…

3+ million open cybersecurity jobs globally!	33% of security teams struggle with turnover
People	
43% of security teams spend most of their time dealing with raw data	82% of alerts an organization receives are not actionable
Processes	
Enterprise security teams manage an avg. of 76 tools	19% of orgs find it impossible to act on their intel
Technology	

OSINT Sources		
News Articles/ Media Reports (nytimes.com)	Phone Directories (whitepages.com)	Contextual Location-related Data (ipfy.org)
Published Research (scholar.google.com)	Court Filings (pacer.uscourts.gov)	Breach Compromise / Disclosure information (privacyrights.org)
Books and Similar References (archiveofourown.org)	Arrest Records (uscourts.gov)	Publicly Shared IoCs (otx.alienvault.com)
Social Media Posts (twitter.com)	Public Trading Data (sec.gov)	Certification Domain / Registration Data (lookup.icann.org)
Consensus Data (consensus.gov)	Public Surveys (statista.com)	Application Systems / Vulnerability Data (nvd.nist.gov)

Hiring Advice for How to Bridge Talent and Expertise Gaps - Focus Areas

1. Retention strategies
2. Efficient talent acquisition process
3. Employee experience
4. Reskilling your workforce in lieu of layoffs
5. Workplace environments
6. Feedback and appreciation
7. Competitive salary and benefits

Baselining Intel Expectations Regarding People, Processes, and Technology

	Early Stage	Maturing	Established
Staff Required	1-2 FTEs ~ $240,000	2-4 FTEs ~ $420,000	3-6 FTEs ~ $630,000
Tool(s)	Free tools, scripts, feeds Social Media Monitoring (~ $60k)	Dark Web (~ $60k) IoC Feed (~ $30k+/feed)	“Heavy” Team Cymru (~ $200k) Passive DNS (~ $100k)
Processes	Nascent	Developing	Evolving
Cost to DIY	$300,000	$520,000	$900,000

DIY intelligence programs will continually struggle to stay ahead of stakeholders when put head-to-head with Managed Intelligence

Who Benefits from Threat Intelligence?

Whether you are a small firm with limited resources or a large organization with vast data and analysts to protect you, **threat intelligence can help you defend your organization with greater accuracy, efficiency, and timeliness.**

Threat intelligence allows security practitioners to make timely and informed decisions to protect their people and assets from dangerous threat actors.

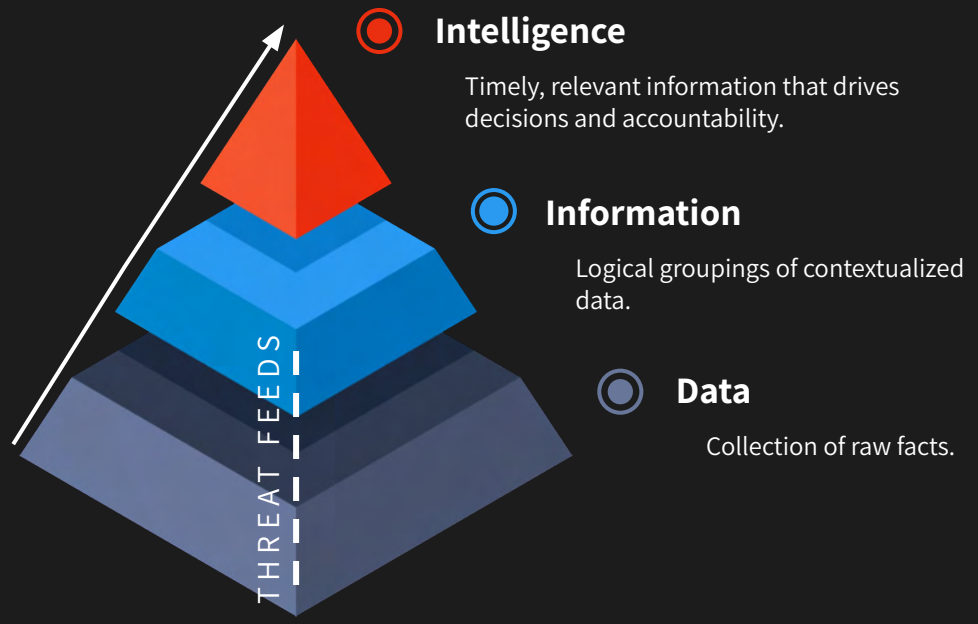
Seven Key Questions Intelligence Helps Answer:

1. Is there an active threat against my organization or key personnel?
2. Who are the people or organizations targeting us?
3. What do those threat actors want?
4. Why do they want to attack us?
5. Which parts of our ecosystem are the most vulnerable?
6. How can we disrupt or mitigate risks based on what we know?
7. Who / what talent do we need to maintain our resilience against attacks?

What Isn't Threat Intelligence?

Threat Intelligence Isn't:

- A feed of broad or industry-focused threat indicators
- Anomaly detection or Artificial Intelligence
- Web, social media, or dark web scanning/scraping
- A visualization platform for all your telemetry



53% of security leaders feel the intelligence they receive from their CTI solutions is not specific enough to their organization.

Maximizing the Value of Intelligence

82% of security leaders feel their threat intelligence is too reactive, leaving teams to respond to breaches after the event instead of before the attack. Security teams want to avoid having to kick into incident response – that's why security controls and clear intelligence requirements can keep you one step ahead of adversaries.

Maximizing the value of open-source information and refining it into actionable intelligence requires a rare combination of skills and experience across a wide array of intelligence domains, including HUMINT, SIGINT, GEOINT, IMINT, and FININT.

For example:

- Geospatial (GEOINT) and imagery (IMINT) intelligence experts can establish a pattern of life from photos posted on social media.
- Online scams on social platforms often point victims to crypto wallet addresses. Financial intelligence (FININT) experts can easily track transactions to and from the address.
- Human (HUMINT) intelligence skills are now practical in cyber space, allowing for direct threat actor engagement, report building, and infiltration of closed forms.
- Signals intelligence (SIGINT) expertise is no longer required to track active flights, as flight data, including aircraft registration, position, altitude, and velocity, are now widely available online.

Nisos is The Managed Intelligence Company™.

Our analyst-led intel investigations, assessments, and monitoring services empower your security, intelligence, and trust and safety teams.

We provide accurate, customized intelligence that guides your security and risk decisions - protecting your organization and people.

Nisos Case Study

How Nisos Threat Landscape Assessments Supported the Intelligence Program Roadmap of a Fortune 500 Company

A major technology company was building an intelligence program and wanted to understand not only the nature of threats targeting the business, but competitors within the industry. They tasked Nisos to conduct a comprehensive Threat Landscape Assessment to help an internal security team level-set and prioritize ongoing intelligence requirements.

Based on our findings, the company chose to:

- Put numerous technical controls in place to reduce the number of hacks.
- Enact a subsequent executive vulnerability monitoring program to reduce executive PII proliferating on the internet.
- Establish a broader social media and dark web monitoring program to quickly identify threats to the business.

Nisos was responsible for evaluating:

1. Digital threats to the company
2. Company sentiments and threats on social media and forums
3. Company information on hacking forums and dark web marketplaces
4. Threats to C-Suite executives
5. Insider threats
6. Threats to subsidiaries
7. Threats to developers
8. Foreign influence campaigns
9. Threats to the wider industry

Nisos Case Study - Results

Intelligence Focus	Discovery
Digital Threats to Company	**Vulnerability discovered:** Nisos found a stale DNS entry that could allow an actor to take control of the IP. **Spoofed International Domain**: An SU TLD using the company trade name was for sale on a Russian-speaking market. **Past Attacks**: Identification of various SQL Injection attempts against company servers, including one anomalous attempt that we recommend be examined more closely.
Social Media and Tech Forums	**Negative Commentary:** Posts on Reddit and Twitter discussed the manipulation of the platform and ways to bypass security controls.
Hacking Forums and Dark Web Marketplaces	**Credentials**: Over 1,000+ company employee email and password combinations were found in 30 breach databases. **Accounts**: Multiple instances of breached company and product line user data, accounts for sale and account checkers, cracking tools, and discussion of 2FA bypass and unban methods.
Threats to C-Suite Executives	**Real Injury:** The CTO was a target for hate language and death threats, some of which referred to attacking him “in real life” or for pay.
Insider Threats and Complaints	**Access:** A few users claimed insider access to proprietary content or tools.
Subsidiaries	**Subsidiary 1:** Physical threats targeting tech convention and instances of a username and password database for sale. Hacker forums also referenced various bypasses, platform abuse, and hacks for sale.
Threats to Developers	**Harassment**: A developer who signed an exclusivity deal with the company was subjected to online abuse and death threats.
Foreign Influence Campaigns	**Asset Risk**: Company assets in Eastern Europe could potentially become exposed to greater Chinese influence, given a significant uptick in Chinese digital infrastructure projects in the area, spearheaded by Huawei. **Theft**: Risks in Shanghai revolve around cybercrime and potential intellectual property theft and government communications monitoring.

Thank You for Watching!

A special thanks to our panelists

Magen Gicinto, Senior VP of People Strategy and Culture, Nisos
Michael Spitzer, Chief Financial Officer, Nisos
Stephen Helm, Product Marketing Director, Nisos

Continue the conversation with us on Linkedin

Follow us on LinkedIn & Twitter @nisos
Subscribe to our blog: nisos.com/nisos-blog/