Gartner Research

CISO Edge: Use Cyber Deterrence to Stop Attacks Before They Start

Will Candrick, Leigh McMullen

29 July 2024

CISO Edge: Use Cyber Deterrence to Stop Attacks Before They Start

29 July 2024 - ID G00803831 - 17 min read

By Analyst(s): Will Candrick, Leigh McMullen

Initiatives: Cybersecurity Leadership; Build and Optimize Cybersecurity Programs

> Common cybersecurity frameworks and best practices overlook an important capability: cyber deterrence. This research explores practical approaches for cybersecurity leaders to develop a cyber deterrence program and stop attacks before they even begin.

Overview

Key Findings

- Gartner reframes "cyber deterrence" as the act of discouraging attackers from targeting an organization by instilling doubt that objectives will be achieved, or a fear of consequences. This differs from common perceptions that deterrence means antagonizing adversaries with "hack back" strategies.

- Existing cybersecurity frameworks and formalized practices emphasize reacting to threats, vulnerabilities, risks and incidents.

- Cyberattackers are rational actors who respond to positive and negative incentives. They seek to achieve their objectives at the lowest cost and with the lowest effort.

- Cyber deterrence remains an overlooked opportunity to mitigate risk because deterrence primarily exists in the realm of national defense and academic debate.

Recommendations

- Define and communicate the concept of cyber deterrence across your organization. Position deterrence as a complement to more established areas of cybersecurity, such as protect, detect, respond and recover.

- Expand cybersecurity's remit to formally include cyber deterrence, and embrace efforts to disincentivize and discourage adversaries before they launch attacks.

- Align deterrence with the rational behavior of cyber criminals using Gartner's PARC Framework as a guide. Adopt a framework that defines attacker motivations and inspires deterrence tactics.

- Create a formal cyber deterrence program that embraces creative thinking and unconventional approaches to cybersecurity. Develop a process to create tactics, identify threat actors, and implement and publicize any new deterrence efforts.

Strategic Planning Assumption

By 2029, 25% of large enterprises will have formally defined and funded cyber deterrence programs to augment traditional cybersecurity measures.

Introduction

C-suites, boards and regulators are more concerned about cybersecurity than ever before. The volume and impact of cyber incidents grows, despite record levels of cybersecurity investment. For example, Gartner finds that cybersecurity spending per employee and as a percent of total IT spend are both at five-year highs, globally, yet the direct and indirect costs of cyber incidents continue to increase. [1]

Cybersecurity leaders' best efforts to mitigate cyber risk still come up short and deliver diminishing returns. Traditional cybersecurity measures, focused entirely on defensive and reactive measures, are built into the frameworks, processes and norms established over the past few decades. These measures are necessary, yet miss novel opportunities to mitigate risk. They only react to new vulnerabilities, patches, attacker techniques, technologies, threats and indicators of compromise (IOCs) — rather than address adversaries before they act.

It's time to proactively impact threats before they're realized. Cyber deterrence offers a compelling, yet often overlooked, addition to traditional cybersecurity measures that augments existing cybersecurity frameworks and models. Although cyber deterrence is not a new concept, few cybersecurity leaders have implemented a formal deterrence program. Gartner offers new guidance and frameworks in this research to help CISOs and their teams turn deterrence discussion and debate into tangible action.

Gartner CISO Edge Series

This content is part of a research series offering leading-edge approaches and guidance to CISOs. This work draws from our work with a small community of thought-leading clients and experts.

Analysis

Define and Communicate Cyber Deterrence to Your Organization and Leaders

CISOs must clearly define cyber deterrence (including what it is and is not), debunk common deterrence myths, and communicate the need for deterrence to senior leaders and stakeholders.

Define Cyber Deterrence

> **"Cyber deterrence" is the act of discouraging attackers from targeting an organization by instilling doubt that objectives will be achieved, or a fear of consequences.**

These deterrence consequences are broadly defined, must remain within legal and regulatory constraints, generally exclude direct "hack back" strategies, and only infrequently involve charges or arrests. To be successful, cyber deterrence programs can — and must — exist within these legal and practical constraints.

Overcome Common Deterrence Myths

Cyber deterrence remains a controversial topic, in part, due to persistent myths. Debunk these common myths to overcome internal objections to defining a sustainable program:

- **Myth: Cyber deterrence means "hacking back."** Cyber deterrence often evokes "hack back" strategies, which are typically illegal and can antagonize, rather than deter, adversaries. **Reality:** Cyber deterrence encompasses many tactics that discourage attackers — such as bug bounty programs, name and shame, honeypots, and ransom payment "claw backs" — without resorting to illegal behavior.

- **Myth: "Proactive" cybersecurity measures offer deterrence.** Most proactive cybersecurity measures, such as threat hunting and continuous threat exposure management (CTEM), only focus on better protection and detection. **Reality:** Cybersecurity programs can discourage adversaries before they even begin attacks, rather than only protecting against and detecting attacks in progress.

- **Myth: Adversaries are relentless and incorrigible.** Cybersecurity professionals continuously experience cyberattacks in progress, and lack insight on potential attacks that are never launched. This creates the experiential bias that cybercrime exists outside the realm of rational behavior. **Reality:** Cyber criminals are people too, and they respond to both positive and negative incentives.

Engage Senior Leaders and Stakeholders

Developing a cyber deterrence program requires internal buy-in and support. This communication must occur within the cybersecurity function and across relevant stakeholders and subject matter experts, such as the CFO, public relations and general counsel.

Many deterrence tactics require collaboration with — and even approval and signoff from — senior leaders and stakeholders. For example, major changes to policy require C-suite approval, public statements need legal signoff and PR support, and new cybersecurity initiatives may require funding.

In these communications, CISOs must standardize how cyber deterrence is defined, debunk common misconceptions, develop processes and secure funding to support deterrence measures.

Expand Cybersecurity's Remit to Formally Include Cyber Deterrence

Currently, deterrence is an overlooked opportunity to mitigate threats and reduce risks. Leading CISOs must counter a few roadblocks that disrupt efforts to adopt cyber deterrence measures. These include:

- **Deterrence Evokes National Security Measures.** Currently, cyber deterrence exists primarily in the realm of national security and academic debate. This perception leads CISOs to believe cyber deterrence is outside the remit of cybersecurity programs.

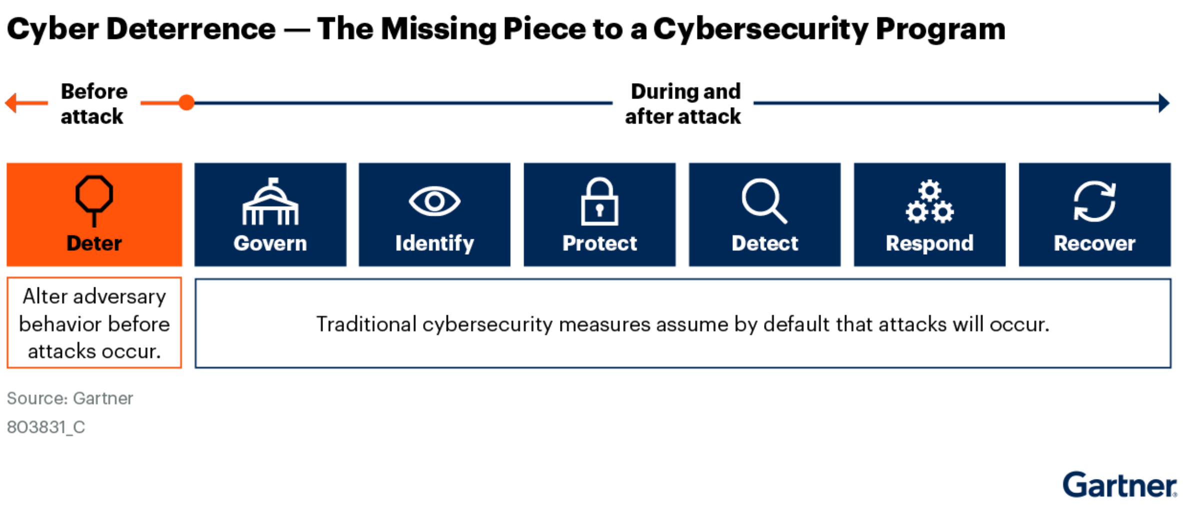
- **Popular Frameworks Omit Deterrence.** Cybersecurity frameworks, such as NIST CSF, NIST 800-53, ISO 27002 and the Cyber Kill Chain, prioritize actions to protect against attacks — and then subsequently detect, respond, recover and generally disrupt malicious actors once an attack occurs. This focus misses opportunities to deter attacks before they occur.

Add Deterrence to Cybersecurity's Remit

Leading CISOs should formally expand cybersecurity's remit to include deterrence. To do this, deterrence must be defined as a stand-alone capability that complements more established cybersecurity measures.

One approach to accomplish this is to add deterrence to existing cybersecurity standards. For example, building off of the popular NIST CSF, deterrence becomes a seventh function. Notably, deterrence serves to alter adversary behavior before attacks occur — and thus, before protection, detection, response and recovery measures are invoked (see Figure 1).

Figure 1: Cyber Deterrence — The Missing Piece to a Cybersecurity Program


Cyber Deterrence — The Missing Piece to a Cybersecurity Program
Before attack
During and after attack
Deter
Govern
Identify
Protect
Detect
Respond
Recover
Alter adversary behavior before attacks occur.
Traditional cybersecurity measures assume by default that attacks will occur.
Gartner

Source: Gartner
803831_C

Cyber deterrence relies on a critical assumption: cyber criminals are rational actors who respond to positive and negative incentives.

Cybersecurity professionals do not condone malicious actions and motivations. Rather, leading cybersecurity leaders recognize that attackers are people too.

Explore Cyber Deterrence in Action

Recent history suggests that cyberattackers generally respond to positive and negative incentives and shift their behavior accordingly. This rational behavior offers an opportunity for cybersecurity leaders to explore and use deterrence to prevent attacks.

Real-world examples of cyber deterrence in action include:

- **Project Fortress Private-Public Collaboration:** More than 800 financial services companies joined the U.S. federal government's Project Fortress. This public-private initiative provides a portfolio of free services to the financial services industry, including protective and even offensive measures, with a view toward deterring adversaries. [2]
- **United Airlines Bug Bounty Program:** United Airlines became the first airline to develop an open and transparent bug bounty program so that hackers can cash in on their exploits — without harming United Airlines or selling exploits to other malicious actors. [3], [4]
- **LockBit Backtracking:** The LockBit ransomware gang apologized and released a free decryption key after being publicly shamed for targeting a children's healthcare organization. This especially egregious attack risked motivating law enforcement and government action beyond that of a typical ransomware attack. [5]
- **Public Exposure Limiting RSA SecurID Breach:** The compromise of RSA SecurID was quickly caught when Lockheed Martin went public with an attack it detected. This quick action essentially burned a zero-day exploit before the attacker maximized ROI. [6]

- **Ransom Payment Clawback:** The FBI recovered $4.5 billion in stolen currency and arrested two individuals who attacked the crypto exchange. The attackers suffered personal legal and financial consequences from their actions. [7]

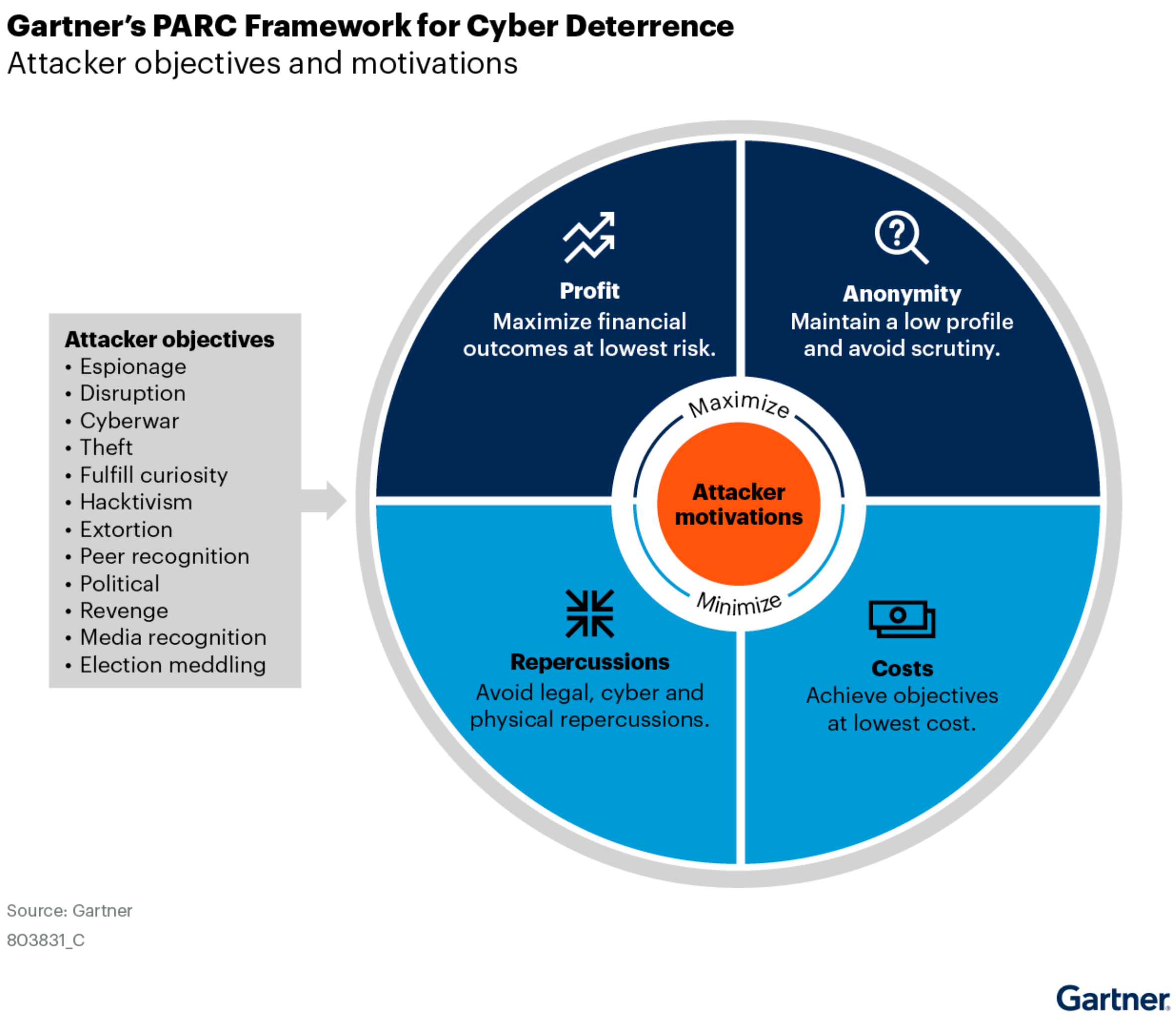
Introducing Gartner's PARC Framework

Deterrence hinges on understanding attackers' motivations and then applying positive and negative incentives to change their behavior. To organize this effort, Gartner developed the PARC (Profit, Anonymity, Repercussions and Costs) Framework (see Figure 2).

The PARC Framework consists of two components:

- **Attacker Objectives:** These are the specific outcomes an attacker seeks. For example, hacktivism can raise awareness for a social cause, and ransomware can generate revenue or data theft to spy on an adversarial nation-state. Other examples include espionage, disruption and cyberwar.
- **Attacker Motivations:** Attacker motivations capture the core needs and priorities of individual attackers or adversarial groups. Attackers are guided by their motivations while pursuing their objectives. Importantly, not all motivations apply equally to all attacker profiles.

Figure 2: Gartner's PARC Framework for Cyber Deterrence



Source: Gartner
803831_C

The four core components of the PARC Framework are:

- **Profit**: Attackers seek to maximize financial outcomes at lowest risk while avoiding scenarios that may have a negative financial outcome.
- **Anonymity**: Attackers seek to maintain a low profile or otherwise avoid scrutiny that impedes objectives.
- **Repercussions**: Attackers seek to maintain their personal, group and/or country's safety from legal, cyber and physical repercussions.
- **Costs**: Attackers pursue the most efficient methods of achieving objectives and prefer to preserve tactics, techniques and procedures (TTPs) to maximize their value.

These motivations help cybersecurity understand attackers, and serve as an organizing principle to develop positive and negative incentives. While deterrence more commonly deploys negative incentives to discourage attack, examples of positive incentives — such as bug bounty programs — are still prevalent.

Create a Formal Cyber Deterrence Program

Mature cybersecurity functions should define a formal cyber deterrence program that complements more established areas of cybersecurity. The CISO must lead this effort, in coordination with general counsel, CFO, public relations, brand protection, law enforcement and any other relevant parties.

CISOs should follow four steps to define and build a cyber deterrence program.

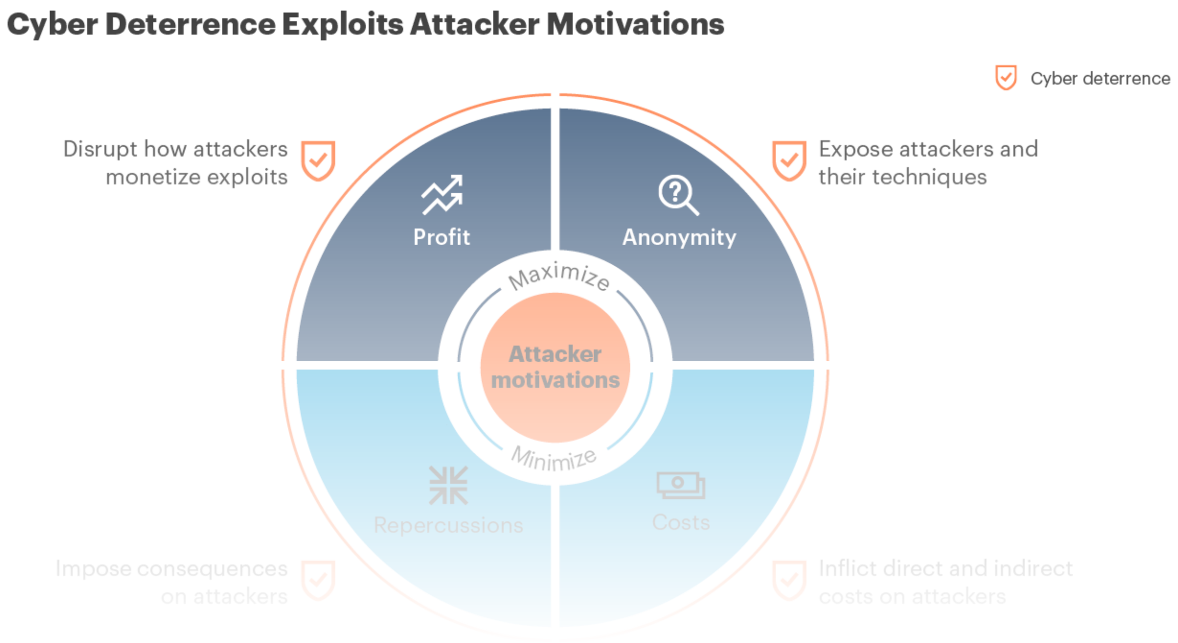
Step 1: Develop Deterrence Tactics

Deterrence tactics are specific actions enterprises can take to exploit attacker motivations and discourage cyberattacks before they even begin. These tactics build upon cybersecurity's understanding of attacker motivations, as established in Gartner's PARC Framework.

Cybersecurity should brainstorm specific tactics that counter or disrupt attacker motivations. These deterrence tactics should achieve at least one of the following deterrence goals (see Figure 3):

- **Profit**: Disrupt how attackers monetize exploits
- **Anonymity**: Expose attackers and their techniques
- **Repercussions**: Impose consequences on attackers
- **Costs**: Inflict direct and indirect costs on attackers

Figure 3: Cyber Deterrence Exploits Attacker Motivations


Cyber Deterrence Exploits Attacker Motivations
Cyber deterrence
Disrupt how attackers monetize exploits
Profit
Anonymity
Expose attackers and their techniques
Maximize
Attacker motivations
Minimize
Repercussions
Costs
Impose consequences on attackers
Inflict direct and indirect costs on attackers

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Report

Cybersecurity Trends: Optimize for Resilience and Performance

Use this report to equip your cybersecurity function for greater resilience.

Download Now

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

eBook

Leadership Vision for Security and Risk Management Leaders

Explore the top 3 strategic priorities for security and risk management leaders.

Download Now

Webinar

Strengthen Your Cybersecurity Leadership to Navigate Evolving Security Landscape

Explore this 5-part series for insights into the evolving landscape.

Watch Now

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight

Gartner®