CYBER DEFENDERS · COUNCIL

DEFEND FORWARD

A Proactive Model for Cyber Deterrence

> "We are all one big blue team..."

STEVE BENTON

EMERITUS CSO AND FORMER DIRECTOR OF PROTECT BT SERVICES & OPERATIONS, BT

Contents

ABOUT

The Cyber Defenders Council

The Cyber Defenders Council is an independent group of preeminent cybersecurity leaders from public- and private-sector organizations around the world. The mission of the Council is to adapt an approach to cyber deterrence, known as "Defend Forward," for private-sector enterprises and to provide prescriptive guidance to help organizations implement Defend Forward cybersecurity strategies that increase costs for attackers and improve the efficacy of Defenders. The Cyber Defenders Council is sponsored by Cybereason.

Executive Summary

Make it **EXPENSIVE** Make it **DANGEROUS** Make it **WORTHLESS**

Those are the design principles around which UK telecommunications provider BT built its security program. The company sought to make it cost prohibitive for attackers to conduct successful attacks, legally perilous for them to try, and to eliminate financial incentives for attackers by making its sensitive data a worthless target.

BT's program captures the spirit of an emerging approach to cybersecurity known as Defend Forward. This approach places increased focus on deterrence, intelligence sharing, and defending with an offensive mindset. As the lines between nation-state sponsored and financially motivated cybercrime attacks continue to blur, and as government officials around the world warn businesses to prepare for cyberattacks stemming from geopolitical conflicts, Defend Forward seeks to empower defenders with the proactive strategies and bias for action they need to confront motivated adversaries.

This report explores the origins and principles of Defend Forward. It captures insights from General Joseph Dunford, the 19th chairman of the US Joint Chiefs of Staff, and showcases recommendations from Cyber Defenders Council members who serve as top security executives and advisors across a range of organizations and industry verticals. Council members met privately in March and April of 2022 under the Chatham House Rule to share their impressions of Defend Forward and discuss ways security leaders can put some of its principles into practice in the private sector.

The Origins of Defend Forward

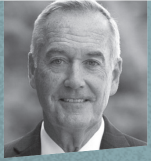
The Defend Forward concept emerged from the US Department of Defense 2018 National Cyber Strategy. Senior Defense Department leaders had grown increasingly concerned about the sophisticated ways in which certain nation-states were bringing together economic coercion, political influence, information operations, cyber operations, and conventional and unconventional military operations to advance their national interests.

The evidence of those nation states' persistent efforts to project power globally and compete with the US in cyberspace showed up in a staggering series of cyber incidents, including interference in the 2016 election, the crippling 2017 WannaCry and NotPetya attacks, the 2017 theft of cyber tools from the US National Security Agency (NSA), corporate intellectual property theft, as well as the massive US Office of Personnel Management and Equifax data breaches.

Because the outcomes from those cyberattacks did not meet the threshold to elicit a traditional kinetic military response, there was little the US government and military could do to intervene proactively. The United States' diplomatic and military posture in the years leading up to 2018 had been to focus on deterrents to cyber aggression and only respond in the event deterrence failed.

Defense Department leaders realized that the kind of adversarial competition in which certain nation-states were engaging demanded new, more proactive and innovative ways of integrating the elements of national power. Defend Forward became the cyber component of a new strategic approach to this competition.

> “On a day to day basis, we were on the sidelines, watching as nation-state threat actors interfered in our democracy and stole priceless trade secrets from our private-sector enterprises. **It became clear to me that if we were going to continue following this military strategy of only reacting in the event deterrence failed, the US was going to find itself at a very significant disadvantage.** I also believed that if our democracy or our nation's critical infrastructure was being threatened, we ought not to be sitting on the bench admiring those problems.”



GENERAL JOSEPH DUNFORD
THE 19TH CHAIRMAN OF THE US JOINT CHIEFS OF STAFF

What It Means to Defend Forward

As described in the Department of Defense Cyber Strategy, Defend Forward means proactively disrupting or stopping malicious cyber activity before it reaches its targets. This approach relies on:

INTELLIGENCE ▶ Collecting intelligence about adversary tactics, techniques and procedures (TTPs).

RESILIENCY ▶ Strengthening the security of systems and networks to make it harder—and more costly—for adversaries to achieve their objectives, and if possible, to deter them from trying.

COLLABORATION ▶ Working closely with peers in law enforcement, across and between industry verticals, and between the public and private sectors to bolster an informed defense that does not include any illegal counter-engagement.

CAPABILITIES ▶ Developing scalable, adaptable, lawful and diverse capabilities for countering adversary actions and activities.

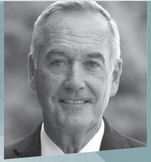
ANALYTICS ▶ Using enterprise cybersecurity solutions to operate at machine speed, combined with large-scale data analytics, to identify malicious activity in its earliest stages across disparate networks and system assets.

Adapting Defend Forward for the Global Private Sector

Defend Forward remains as relevant a cybersecurity strategy today as it was in 2018, especially as the world braces for cyberattacks stemming from the conflict between Russia and Ukraine. While the Department of Defense definition of Defend Forward includes offensive activities in which private sector enterprises cannot engage, there is much for the private sector to glean from both the proactive "take the fight to the adversary" perspective and the focus on deterrence.

"If our adversaries are going to be persistent in cyberspace every day, and if we continue to rely on a passive, firewall mindset, we'll never be successful against them," says General Dunford.

“Defend Forward doesn’t have to mean hacking back, but it does mean acting proactively and with purpose—on the basis of intelligence—to anticipate and disrupt threats. **It’s about putting attackers on their heels instead of defenders getting caught by surprise.** It’s about defending with an offensive mindset, and an offensive mindset is not illegal.”



GENERAL JOSEPH DUNFORD
THE 19TH CHAIRMAN OF THE US JOINT CHIEFS OF STAFF

Growing Support for Proactive Deterrence

Leading global organizations are already moving in the direction of adopting Defend Forward principles. For example, Philipp Amann, the head of strategy at the European Cybercrime Centre (EC3), says Defend Forward aligns with the proactive, deterrence-focused approach supported by EC3 in dealing with cyber adversaries. As examples, Amann cites the regulatory and technology watch function that EC3 established in 2013 to assess the ways in which malicious actors could abuse emerging technologies, along with the No More Ransom initiative that helps organizations recover their data without paying a ransom to attackers.

Similarly, the security program at BT is built around three objectives aimed at deterring attacks, according to Steve Benton, emeritus CSO of BT and former director of Protect BT Services & Operations:

Make it

EXPENSIVE
for an adversary to wage a successful attack on the company.

Make attacks

DANGEROUS
for adversaries via a strong digital forensics team capable of gathering evidence that allows law enforcement partners to identify actors and bring them to justice.

Make attacks

WORTHLESS
to adversaries by encrypting valuable data at rest or in motion and taking proactive steps to protect customers from fraud.

The Six Principles of Defend Forward

1 ASSUME YOU'RE AT RISK

2 UNDERSTAND THE THREAT

3 COLLABORATE ACROSS SECTORS

4 USE INTELLIGENCE TO INSTILL A BIAS FOR ACTION

5 LEVERAGE LARGE-SCALE ANALYTICS AND TECHNOLOGY TO THE GREATEST EXTENT POSSIBLE

6 ASSUME YOU'RE STILL AT RISK

1

PRINCIPLE ▶ ASSUME YOU'RE AT RISK

It isn't difficult for security leaders to predict the kinds of incidents that can put their organizations at risk, but Council members admit that convincing their organization's senior leadership to invest in preparing for a range of scenarios, including the more rare "black swan" events, can be difficult. They note it often takes a significant security event to get business executives to take cybersecurity seriously.

Since Council members don't want to wait for another attack that rises to the level of NotPetya or Colonial Pipeline (or worse), they recommend that industry organizations, such as ISACs and the Cyber Defenders Council, do the kind of scenario planning that industry group SIFMA does for the securities industry with its Quantum Dawn cyber war gaming exercises. They agree having a third-party organization play out and report on these scenarios could help CISOs make stronger, more credible business cases to their leadership teams.

One significant yet frequently underestimated risk that Council members say security leaders and their executive teams need to better prepare for is the risk startups and smaller organizations create for the larger organizations they serve. They note smaller companies lack the security maturity of many large enterprises, and that startups tend to have a much greater appetite for risk than larger companies.

"Until large and small companies align on a standardized approach to security, the gap between their maturity and capabilities will only increase, and the more large companies will experience security incidents as a result of smaller partners in their ecosystems," says Nils Puhlmann, a co-founder of the Cloud Security Alliance and a veteran technology industry CISO.

Using open-source software can present similar risks, as the Log4j vulnerability demonstrated in December 2021 and beyond. To prevent more Log4j-type supply chain issues in the future, Council members encourage security practitioners to provide more feedback to the open-source community in a consistent and systematic way. They specifically recommend that application security resources devote some of their time to looking at open-source code and reporting potential vulnerabilities. Mike Orosz, vice president of information and product security at Vertiv, suggests that it may be time for the platforms hosting open-source code to create terms and conditions that state that in exchange for using their software for free, users agree to report back on any vulnerabilities they find, along with potential solutions.

Alex Schuchman, CISO for Colgate-Palmolive Company, recommends using tools that validate open source libraries, check for vulnerabilities and dependencies, and provide curated repositories from which to pull code. Some tools that perform those activities include Node Security Project, Gemnasium, Source Clear, Protecode and Sonatype.

2

PRINCIPLE ▶ UNDERSTAND THE THREAT

Defend Forward security strategies hinge on organizations having a keen understanding of the attackers most likely to target them, the reasons those attackers would want to compromise them, and the methods they'd be most apt to use, including the network security, application security, and supply chain security weaknesses they could exploit. Since adversaries have so many vulnerabilities at their disposal, prioritizing vulnerabilities becomes an extremely important component of proactive defense.

Council members note that participating in classified government threat intelligence programs can give organizations visibility into threats and threat actors they wouldn't otherwise get. Although organizations would need to put certain policies and controls in place to obtain the security clearances required to participate in those programs, taking such steps is increasingly necessary, especially for organizations operating in critical infrastructure sectors, as those sectors face heightened threats from nation-state actors.

> “By understanding how our adversaries are trying to target us, we can be more focused in our defense instead of trying to protect all things equally.”

RICARDO LAFOSSE
CISO OF THE KRAFT HEINZ COMPANY

3 PRINCIPLE ▶ INTELLIGENCE SHARING AND COLLABORATION

Council members agree that collaboration and intelligence sharing across industries and with the federal government, CSIRTs, and academic institutions is critical to understanding and proactively addressing threats. The drawback: information sharing remains fraught with challenges. Some of the biggest barriers include protecting confidentiality, especially in smaller markets like Korea and Malaysia, and building and maintaining trust.

"Nobody wants to share potentially embarrassing experiences," says Hoo Ming Ng, former deputy chief executive for Singapore's Cyber Security Agency.

Building trust–both within and across industries, and between the public and private sectors–obviously takes time, but information sharing groups can facilitate it with policies and processes designed to protect anonymity. For example, Council members representing ISACA Singapore and the Global OT-ISAC say their organizations' Safe Harbor provisions have fostered greater openness among their members by granting a degree of anonymity along with some liability protection.

In addition, the OT-ISAC supports machine-to-machine sharing mechanisms that leverage Traffic Light Protocol (TLP) and anonymous submissions. The OT-ISAC has also established different classifications for sharing that include: restricted information that can only be shared with a proscribed group; confidential information that may only be shared within a specific community; information that can be shared among general OT-ISAC members, with other groups, and with government partners; and information that can be shared freely with the public.

Despite industry groups' efforts to build trust and make their participants and the organizations they represent feel confident in sharing sensitive intelligence, several Council members say their organizations' corporate policies, intended to reduce their legal exposure, limit the information they are allowed to share. To overcome this particular hurdle, they say there is a need to show that the costs of not sharing intelligence on cyberattacks outweigh potential legal and reputational risks associated with sharing. Reports on the cost of data breaches from public filings with the US Securities and Exchange Commission (SEC) may help security leaders make this case. Global regulators also need to address conflicts between laws that penalize organizations for breaches and other laws intended to encourage sharing.

Globally, Council members concur that policy and financial incentives are needed to promote collaboration across the private sector and with public sector entities. Market forces, like contractual terms with vendors and suppliers, along with cyber insurance coverage models, may also serve to foster collaboration and intelligence sharing.

As intelligence sharing increases, Council members say platforms are needed to deconflict different sources of intelligence and help prioritize actions–e.g., for high risk threats, organizations should focus on investigation, deterrence and disruption, and for low risk threats, organizations can focus on prevention and awareness.

> “I want to be in a world where companies can be more transparent about security incidents and where that kind of transparency doesn't invalidate or cancel a company. We need to resist the impulse to bayonet the wounded.”

SAM CURRY
CSO, CYBEREASON

4

PRINCIPLE ▶ USE INTELLIGENCE TO INSTILL A BIAS FOR ACTION

Council members say threat intelligence should drive a wide variety of strategic and tactical security decisions short of offensive activities, and they encourage all security practitioners to incorporate actionable threat intelligence into their day to day actions and decision-making as much as possible. Robert Oh, the executive vice president, head of corporate digital strategy and COO of Doosan Digital Innovation, says having the right processes in place to synthesize and deploy threat intelligence is critical. It's also critical to consult with relevant law enforcement officials before taking any response actions that may inadvertently create legal or regulatory risks.

Design goals based on intelligence can help security leaders instill a bias for action among themselves and their teams. These goals clarify the threat actors that security teams are trying to protect their companies from, as well as the level of resources and sophistication an organization anticipates an adversary would dedicate to an attack.

"Design goals drive a level of accountability for achieving specific security and business resiliency outcomes," says Malcolm Harkins, chief security and trust officer for Epiphany Systems. "Design goals help security leaders and their teams identify everything they need to put in place from a people, process and technology perspective. Security leaders can then use penetration testing and other exercises to determine whether or not they're achieving those goals."

Threat intelligence isn't only important to security teams. Beth-Anne Bygum, senior vice president and chief security and compliance officer at Acxiom, and BT emeritus CSO Steve Benton recommend getting threat intelligence into the hands of business people, especially those working in governance, risk and compliance (GRC) functions, so they can make risk-intelligent business decisions and take proactive measures every day to reduce their organization's exposure.

For example, Bygum recommends that GRC teams apply threat intelligence to contract negotiations with vendors. If GRC teams know vulnerabilities in certain vendors' software are leading to breaches, they know to incorporate "right to audit" clauses into contracts. "When I have vendors who are not patching or keeping their code current, I call on that right to audit and to have CISO to CISO conversations between myself and the vendor because of the potential supply chain issues the lack of patching could create," Bygum says.

Getting teams to act on intelligence takes a concerted effort, and sometimes, culture change. While serving as the 36th Commandant of the Marine Corps, General Dunford took creative steps to build a culture of intelligence sharing. He went so far as to have posters made in his organization that posed the following questions: What do I know? Why is it important? Who else needs to know about it? Have I told them? What needs to be done with this information? Who needs to do it? Did they do it? "These are the kinds of things that are required to move people beyond the passive state of receiving intelligence to actually do something with it," he says.

BUILDING A CULTURE OF INTELLIGENCE SHARING

Key Questions Security Teams Can Ask Themselves Every Day

- What do I know?
- Why is it important?
- Who else needs to know about it?
- Have I told them?
- What needs to be done with this information?
- Who needs to do it?
- Did they do it?

5

PRINCIPLE ▶ LEVERAGE LARGE-SCALE ANALYTICS AND TECHNOLOGY TO THE GREATEST EXTENT POSSIBLE

Large-scale analytics capabilities hold the promise of enabling security teams to address one of their biggest challenges: the fact that they are drowning in data and alerts that do not rise to the level of actual intelligence. The downside is that this infrastructure and these capabilities do not come cheap. What's more, according to a survey of IT and cybersecurity leaders conducted by CIO Academy Asia, many organizations lack the mature data management capabilities required to fully leverage artificial intelligence and machine learning at scale for threat hunting, early detection and automated response.

On the upside, vendors and services providers are increasingly building this infrastructure and hosting it on behalf of clients to make it more accessible to more organizations. The more organizations have access to advanced analytics, the more they can gain an operation-centric view of malicious activity on their systems and networks, and the more effectively they can use behavioral indicators to proactively spot and stop suspicious activity in its earliest stages, before it leads to business impact.

6

PRINCIPLE ▸ ASSUME YOU'RE STILL AT RISK

Council members have shown how a Defend Forward mindset and approach can help security leaders build robust programs for their organizations that drive accountability and deliver meaningful business and cybersecurity outcomes. Although Defenders may never be able to completely deter cyberattacks, especially those that are nation-state sponsored, if we collectively do the equivalent of identifying the "doors and windows" that adversaries are likely to exploit, lock them down, and put pressure on third-party partners to do the same, we'll have more than a fighting chance to all but eliminate opportunistic and financially motivated attacks and curtail the risk posed by nation-state sponsored operations as well.

NORTH AMERICA/EMEA COUNCIL MEMBERS

PHILIPP AMANN
HEAD OF STRATEGY - EUROPEAN CYBERCRIME CENTER, EUROPOL

STEVE BENTON
EMERITUS CSO - FORMER DIRECTOR OF PROTECT BT SERVICES AND OPERATIONS, BT

PAUL BIVIAN
DIRECTOR OF INFORMATION SECURITY, KIRKLAND & ELLIS LLP

KEVIN BROWN
CISO, SAIC

BETH-ANNE BYGUM
SVP - CHIEF SECURITY AND COMPLIANCE OFFICER, ACXIOM

ROLAND CLOUTIER
GLOBAL CSO, TIKTOK

SAM CURRY
CSO, CYBEREASON

JOSEPH DUNFORD
19TH CHAIRMAN OF THE JOINT CHIEFS OF STAFF

RENEE GUTTMANN
EMERITUS CISO, TIME WARNER AND THE COCA-COLA COMPANY

MALCOLM HARKINS
CHIEF SECURITY AND TRUST OFFICER, EPIPHANY SYSTEMS

PETER KUNZ
DIVISIONAL CISO, LEICA GEOSYSTEMS

RICARDO LAFOSSE
CISO, THE KRAFT HEINZ COMPANY

JANET LEVESQUE
CISO, ATHENAHEALTH

NORTH AMERICA/EMEA COUNCIL MEMBERS

DAVE LEWIS
GLOBAL ADVISORY CISO, CISCO

DR. YONESY F. NÚÑEZ
CISO, JACK HENRY & ASSOCIATES

MIKE OROSZ
VP INFORMATION/ PRODUCT SECURITY, VERTIV

THERESA PAYTON
CEO, FORTALICE, AND FORMER WHITE HOUSE CIO

CHRISTOPHER PETERS
VP AND CSO, ENTERGY

NILS PUHLMANN
CO-FOUNDER, CLOUD SECURITY ALLIANCE

ALEX SCHUCHMAN
CISO, COLGATE-PALMOLIVE COMPANY

KERISSA VARMA
MANAGING EXECUTIVE - CYBERSECURITY, VODACOM

ERIK WILLE
CISO, AMERICAN AXLE & MANUFACTURING

ASIA-PACIFIC COUNCIL MEMBERS

HOO MING NG
FORMER DEPUTY CHIEF EXECUTIVE, CYBER SECURITY AGENCY OF SINGAPORE

CHARLES NG
EVP - INTERNATIONAL BUSINESS & CONSULTING, ENSIGN INFOSECURITY

KEITH LEONG
MANAGING DIRECTOR - GLOBAL DELIVERY, NCS

CHUAN WEI HOO
GROUP CISO, ST ENGINEERING

PEI YUEN WONG
CTO, IBM SECURITY

SENG WEI KENG
CISO, DBS BANK

EUGENE TEO
VP AND DEPUTY CSO, ULTIMATE KRONOS GROUP (UKG)

YUEZHONG BAO
CISO, LAZADA GROUP

BORIS HAJDUK
CISO, TOKOPEDIA

MICHAEL BECERRA
CISO, DHL EXPRESS

PAUL LEK
DIRECTOR - IT RISK MANAGEMENT & SECURITY APJ, MSD (MERCK & CO.)

LEONARD ONG
APAC CISO, GE HEALTHCARE

CHRISTOPHER LEK
DIRECTOR CYBER SECURITY, NANYANG TECHNOLOGICAL UNIVERSITY

SHAO FEI HUANG
PRINCIPAL SECURITY ARCHITECT, AWS

STEVEN SIM KOK LEONG
PRESIDENT, ISACA SINGAPORE

JOHN LEE
MANAGING DIRECTOR - APAC, GLOBAL RESILIENCE FEDERATION & OT-ISAC

JOHNNY KHO
PRESIDENT, ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS

ASIA-PACIFIC COUNCIL MEMBERS

SHIH HSIEN LIM
CISO AND CSO, CERTIS

JASON WONG
GLOBAL HEAD OF IT SECURITY & COMPLIANCE, DYSON

DATO' TS. DR. HAJI AMIRUDIN ABDUL WAHAB
CEO, CYBERSECURITY MALAYSIA

SHANKAR KRISHNAN
CISO, AXIATA DIGITAL SERVICES & BOOST MALAYSIA

ANGEL REDOBLE
GROUP CISO, PLDT & SMART COMMUNICATIONS

MEL MIGRIÑO
GROUP CISO, MERALCO (MANILA ELECTRIC COMPANY)

YARON SLUTZKY
CSO, AGODA

ROBERT OH
EVP - HEAD OF CORPORATE DIGITAL STRATEGY & COO OF DDI BU HEADQUARTERS, DOOSAN

JOHN TAYLOR
GROUP CIO - TECHNOLOGY & SECURITY, MEDHEALTH

JASON LAU
CISO, CRYPTO.COM

DENNY HUSEN
GLOBAL HEAD OF INCIDENT RESPONSE, CRYPTO.COM