

Xenon Partners

Xenon Advisory

Cyber Security Edition

サイバーセキュリティ版

Q2 2019

¥4900

XENON ADVISORY

Xenon Advisory, Xenon Partners' advisory arm, specializes in cyber security and developing software with security in mind. Xenon itself began as a bootstrapped funded private equity company focused on Business-to-Business Software as a Service (B2B SaaS), and grew through its successes to become the well resourced private equity firm it is today.

With its expertise in software, Xenon felt the need to leverage its skill set to not only build good products, but secure products. As part of that mission, Xenon developed a specialized cyber security team comprised of experts skilled in both engineering and protecting software to leverage across its portfolio companies.

In this magazine, in hopes of helping the cyber world become a safer, more secure environment, we seek to share our expertise and inform IT professionals, business executives, and other relevant stakeholders regarding the urgency and importance of cyber security today.

Xenon Partnersの勧告部門を担うサイバーセキュリティ専門のXenon Advisoryは、セキュリティを念頭にソフトウェアを開発している。Xenon社自体は「サービスとしての企業間取引ソフトウエア」に注力した自己資金未公開株式会社として開始し、成功を成し遂げて成長した。そして、資金源が豊富な未公開株式投資会社として今日に至る。

Xenon Advisoryは、すばらしい製品を構築するだけでなく、セキュリティ製品の開発に、ソフトウェアに特化するXenonはスキルを活用すべきだと感じている。その使命の一部として、Xenonは専門サイバーセキュリティチームを結成した。ポートフォリオ企業に活用するソフトウェアのエンジニアリングと保護の両方のスキルを備えたエキスパートチームである。

本誌では、サイバーの世界がより安全な環境になることを願い、当社の専門知識を共有し、IT専門家、事業経営者、およびその他関連利害関係者に、今日のサイバーセキュリティの緊急性と重要性に関する情報を提供する。

“Cybersecurity is now, more than ever, a state of mind. Responsibility lies not in one team, but throughout an entire organization.”

– Jonathan Siegel, Chairman of Xenon Partners

「 サイバーセキュリティはいまや、一種の精神状態となりつつある。
責任は1つのチームではなく組織全体に存在するのだ。」

- Xenon Partners会長　Jonathan Siegel

TABLE OF CONTENTS

In The News

Bits & Pieces from around the Globe 7
Yet Another (Sly) Bitcoin Hack 11
The Hidden Cost of a Data Breach 13

TBT: Trends, Breaches, and Threats

Emotet: Dissecting a Trojan Horse 16
Security Trends for 2019 and Beyond 20
The OPM Hack: When “Tony Stark” Took on the U.S.A. 24

Taking Action

Securing Open Source Code 29
The Human Factor: How the Pentagon Looked to High Reliability Organizations to Win at Cyber Security 38

ニュース

世界ニュースダイジェスト 7
さらにもう一つの（陰険な）ビットコインハッキング 11
データ侵害の隠れたコスト 13

TBT：動向、侵害、および脅威

Emotet：トロイの木馬を分析 16
2019年以降のセキュリティ動向 20
OPMのハッキング：「トニー・スターク」のアメリカ進出 24

行動を起こす

オープンソースコードの保護 29
サイバーセキュリティにおいて高信頼性組織（HRO）になる 38



IN THE NEWS

Whether it be a new data breach or hacking attempt, cyber security incidents occur almost every day throughout the globe. From Bitcoin theft, to the unseen and unsavory costs that often go unaccounted for when facing data breaches, new developments are constantly unfolding. Hackers, security experts, risk, and technology all change and evolve simultaneously, which contributes to the challenge. Keeping up to date on these breaches and ensuring excellent cyber security remains top of mind for organizations across the world; it has and will continue to be pivotal to ensure security.

新たなデータ侵害やハッキングの試みに関係なく、サイバーセキュリティに関する事件は世界中でほぼ毎日発生している。 ビットコインの盗難から、データ侵害における多くの原因不明な予測できない不快なコストに至るまで、新たな展開が絶えず明らかになっている。ハッカー、セキュリティの専門家、リスク、テクノロジーはすべて同時に変化・進化している。これが課題の一因となっている。常にこれらの侵害に関する最新の情報に目を向け、優れたサイバーセキュリティを確保することは、依然として世界中の組織にとって最優先事項である。今昔問わず、このことはセキュリティを確保する上で極めて重要なことだ。

Bits & Pieces from Around the Globe

Increasing Risk to Banking Sector
Recently, at the World Economic Forum, leaders from around the globe participated in a panel discussion of ways to prevent and mitigate another financial crisis. Japan's central bank chief, Haruhiko Kuroda, pointed to cyber-risks potentially becoming the financial system's greatest risk in the coming years.

Cyber Risks Cause Greater Economic Impact Than Potential Trade War, According to Estimates
With many headlines over the past year focused on the evolving trade barriers and looming trade wars, trade tensions are relatively well-known compared to other large-impact items such as cyber-crime. However, both trade and cyber issues have received wide attention from investors and companies, who consistently point to both risks being among their primary concerns.

According to reporting by the Center for Strategic and International Studies as well as McAfee, the world-wide cost of cyber crime is just shy of $600 billion annually. This accounts for up to a 0.7 percent loss in global gross domestic product, or GDP (calculated according to the International Monetary Fund's measuring practices). Comparatively, the IMF estimates that the impact of a trade war would manifest in a reduced global GDP as well. Specifically, the IMF calculates, the trade war would reduce global GDP by 0.5 percent by 2020, which can be crudely estimated at around $450 billion.

While the impacts of the trade war should not be understated, cyber crime, especially given its devastating economic impact, may deserve as much or more attention than fear over potential trade war damages.

世界ニュースダイジェスト

銀行部門のリスク増大
最近、世界中の指導者達が世界経済フォーラムにて、今後の金融危機を予防・緩和する方法に関するパネルディスカッションに参加した。そこで日本銀行総裁の黒田東彦氏は、サイバーリスクが今後数年間で金融システムの最大のリスクになる可能性があると指摘した。

サイバーリスクは潜在的な貿易戦争を超える経済インパクトがあるとの推計結果
徐々に発展している貿易障壁と迫りくる貿易戦争に注目しているニュースの見出しがこの1年間で多数見られる。サイバー犯罪のような他に大きな影響を与える内容と比較すると、貿易障壁は比較的より知られている。一方、貿易およびサイバー問題が投資家や企業から広く注目されており、一貫してこの2つのリスクが最大の関心事であると指摘されている。

戦略国際研究センターおよびMcAfeeによる報告から、世界規模のサイバー犯罪の費用は年間6,000億ドル弱にのぼっている。これは、世界の国内総生産（GDP－IMFの指標に従って計算される）の最大0.7%の損失に値する。IMFは、割合的に貿易戦争のインパクトが世界のGDPの減少としてはっきり表れると推定している。具体的には貿易戦争が2020年までに世界のGDPを0.5%削減し、この額がおよそ4500億ドルになると推定されている。

貿易戦争の影響は過小評価されるべきではないが、特にこの壊滅的な経済インパクトを考慮すると、サイバー犯罪は潜在的な貿易戦争の損害に対する懸念以上に注目すべき内容だ。



Israel Amidst A 3-Year Push To Boost It's Cyber Security Industry

In August, the Israeli government said it would invest $24 million to help develop its cyber security industry. Israel plans to boost cybersecurity through this investment into a 3-year program which involves companies participating in high-risk research and development. At the time of the program's announcement, Israel was second only to the United States in the global cybersecurity market share, with 5% of the global market and 16% of cyber industry investment worldwide, according to Israeli government data.

イスラエルのサイバーセキュリティ業界の強化三ヵ年が6か月目に突入

8月、イスラエル政府は、サイバーセキュリティ業界の発展を支援するために2400万ドルを投資すると発表した。イスラエルは、ハイリスクの研究開発に携わる企業を巻き込んだ3年間のプログラムへの投資を通してサイバーセキュリティーを強化する計画だ。同政府のデータによると、このプログラムの発表時点では、イスラエルは世界のサイバーセキュリティ市場シェアで米国に次いで2位、世界全体の5%、そしてサイバー業界への投資の16%を占めている。

Cyber Attack Hits France's Altran

According to news reports, France's Altran Technologies, an engineering consultancy, suffered a cyber attack on January 24th, 2019. Some of Altran's clients include the French utility company Engie, the U.S. satellite operator Iridium, and Britain's Network Rail.

This attack, the latest in an evolving trend of cyber disruptions targeting private businesses, demonstrates an alarming pattern in which both criminals and foreign governments have aggressively launched cyberattacks in recent years.

サイバー攻撃がフランスのAltranを攻撃

ニュース報道によると、2019年1月24日に、フランスの技術コンサルティング企業であるAltran Technologiesがサイバー攻撃を受けた。同企業の顧客には、フランスの公益事業会社であるEngie、米国の衛星通信事業会社であるIridium、および英国のNetwork Railが含まれている。

この攻撃は、民間企業を標的として混乱を引き起こすという最近見られている動向であり、近年では犯罪者と海外政府の両方が積極的にサイバー攻撃を仕掛けるという警戒的なパターンを示している。

U.S. Director Of National Intelligence Highlights Chinese & Russian Cyber Espionage

Recently, U.S. Director of National Intelligence, Dan Coats, testified that China and Russia pose the greatest cyber attack threats to the United States and are becoming increasingly aligned. In his January 29th, 2019 testimony to the U.S. Congress, Coats said that China and Russia continue to erode established security norms and increase the risk for regional conflicts, especially in the Middle East and East Asia, as they seek to expand their global influence.

米国の国家情報局長が中国・ロシアのサイバースパイ活動について強調

最近、米国国家情報局長のダン・コーツ氏は、中国とロシアが米国にとって最大のサイバー攻撃の脅威になっており、提携の強化が進んでいると証言した。2019年1月29日の米国議会に対する証言で、コートは、中国とロシアは特に中東と東アジアで、確立された安全保障規範を侵害し、地域紛争のリスクを増大させ続けていると述べた。

Australian Political Parties Hit By Cyberattacks

In early February 2019, Australian Prime Minister Scott Morrison revealed that Australia's main political parties suffered a cyber-attack launched by a sophisticated state actor. Although which state actor or actors involved were not identified, experts listed China or potentially Russia as likely attackers.

Although the extent and impact of the attacks has yet to be confirmed, this latest cyber attack follows a string of hacking in recent years including attacks on the Australian government's statistics and weather agencies.

Google Seeks To Highlight Deceptive Website Domains

An increasing trend in cyberattacks is the use of fake domains that imitate well known websites, but with slight variations that may go unnoticed by users. To combat this problem, which is on the rise, Google is developing a tool allowing Chrome to warn users when domains appear to use subtle ways to make users believe they are a website they are not.

Japan to Hack Home Devices to Test Cybersecurity Flaws

Starting in mid-February 2019, the Japanese government began an effort to attempt to randomly break into devices located in homes and offices in order to better ascertain vulnerabilities. This cybersecurity effort, conducted via the National Institute of Information and Communications Technology, means the Japanese government will begin actively hacking into devices belonging to Japanese citizens—a first-time practice. The Institute has promised that any data obtained during this process will not be leaked in any way, in order to preserve citizens' constitutional right to privacy.

オーストラリアの政党がサイバー攻撃で打撃

2019年2月上旬、オーストラリアのスコット・モリソン首相は、オーストラリアの主要政党が、高度なハッカーによりサイバー攻撃を受けたことを明らかにした。どのハッカーが関与していたかは特定されていないが、専門家らは中国、あるいはロシアの可能性が高いとみている。

攻撃の範囲と影響はまだ確認されていないが、この最新のサイバー攻撃は、オーストラリアの統計や気象機関への攻撃等、近年の一連のハッキングに続いている。

グーグルが紛らわしいウェブサイトドメインの捜索に注力

サーバー攻撃の増加傾向として、よく知られているウェブサイトを模した偽ドメインの使用が挙げられる。偽ドメインと本物との違いはわずかなため、ユーザーに気づかれにくい傾向がある。この増加している問題に対処するため、グーグルは、偽のウェブサイトをユーザーに本物と信じさせないために、Chromeがユーザーに警告するツールを開発している。

日本がホームデバイスをハッキングしてサイバーセキュリティの欠陥をテスト

2019年2月中旬から、日本政府は脆弱性をより良く確認するために、家庭やオフィスにあるデバイスに作為的に侵入しようとする試みを開始した。独立行政法人情報通信研究機構を通して実施されているこのサイバーセキュリティの取り組みは、日本政府が日本国民の有している機器に初めて積極的にハッキングすることを指す。当機関は市民の憲法上のプライバシーの権利を保護するために、この過程で得られたいかなるデータも決して漏洩することはないと約束している。

Stealing From Apple And Getting Caught

For the second time in 6 months, a Chinese national working for Apple has been arrested for stealing the tech giant's intellectual property. Apple first started investigating employee Jizhong Chen when a co-worker noticed him taking pictures around the workplace. The arrest occurred the day before Chen was scheduled to return to China. Examining Chen's computer, Apple found thousands of files deemed confidential, ranging from manuals to schematics and diagrams of the company's tech secrets.

Allegedly, Chen had applied to work for XMoters, a Chinese company focused on autonomous cars. The Xpeng G3, XMoters' first electric SUV, appears very similar to Tesla's Model 3.

アップルから窃盗を理由に逮捕

アップル勤務の中国人従業員は、技術で最大手企業の知的財産を盗んだとして過去6か月で2回目の逮捕となった。従業員のジージョン・チェン氏が職場で写真を撮っていることに同僚が気が付いことからアップルは調査を開始した。チェン氏が、中国に戻る前日に逮捕された。チェン氏のコンピューターを調べたところ、企業のマニュアルから回路図、そして図表を含む何千もの機密ファイルが発見されました。

伝えられるところでは、チェン氏は中国企業で自動走行車に注力しているXMotersに就職を希望していた。XMotersの最初の電気SUV、Xpeng G3はテスラのモデル3と酷似している。

Yet Another (Sly) Bitcoin Hack

A sly attack on Electrum Bitcoin wallets has earned an unidentified hacker or hacking organization over $750,000. In late December 2018, hackers managed to display a message on Electrum wallet applications asking users to download a wallet update from an unauthorized GitHub repository.

さらにもう一つの（陰険な）ビットコインのハッキング

エレクトラムビットコインウォレットへの陰険な攻撃により、正体不明のハッカーは75万ドルを得ていた。2018年12月下旬、ハッカーはエレクトラムウォレットアプリケーション上でユーザーに、未認可のGitHubリポジトリからアプリのアップデートを促すメッセージを表示した。

FIG. 1



The attack began with the hackers adding dozens of nefarious servers to the Electrum wallet network, then answering transactions that occurred via these servers with an error message asking users to download the (fake) application update from the GitHub repository. Users who downloaded the malicious update were then prompted to use two-factor authentication when they opened their wallets. Previously, two-factor authentication (2FA) was deployed when sending funds and not during the onset of the wallet's launch. However, by exploiting the 2FA code sent to users, the "updated" electrum wallets then transferred funds from the user to the attacker's Bitcoin address.

Hackers were exploiting the fact that Electrum servers were permitted to create popups featuring custom text within user wallets. At first, the attack popups were

この攻撃は、ハッカーがエレクトラムウォレットネットワークに何千もの不正なサーバーを追加することから始まり、このサーバーを経由したトランザクションに対し、GitHubレポジトリから（偽の）アプリケーションのアップデートをダウンロードするように求めるエラーメッセージを表示する内容だ。この悪意のあるアップデートをダウンロードしたユーザーは、ウォレットを開く際に使用する二要素認証（2FA）を使用するよう求められる。従来、2FAはウォレットの販売時ではなく、送金時に求められていた。しかし、ユーザーに送信された2FAコードを悪用することにより、「アップデートされた」エレクトラムウォレットがユーザーから攻撃者のビットコインアドレスに資金を送金する。

ハッカーは、エレクトラムサーバーがユーザーウォレット内にカスタムテキストを含むポップアップの作成が許可されていた事実を悪用した。当初、攻撃ポップアップは、リッチテキスト（図2を参照）で表示されていたため高い信頼性があった。しかし、このポップア

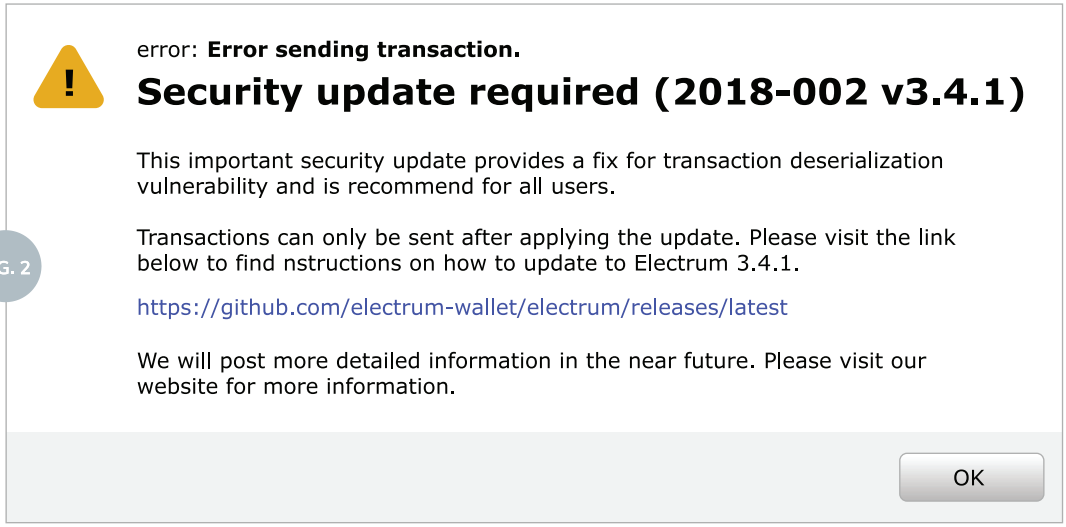


FIG. 2

in rich-format text (see fig. 2), creating a greater sense of authenticity. The popups were accompanied with a clickable link for downloading the nefarious and false update, which enabled the attackers to steal users' Bitcoins. The Electrum team first responded by updating the wallet application so messages could no longer be rendered in rich HTML text (see fig.3). That said, some users continued to fall for the trap laid out by the assailants. Despite the popup not containing a direct link to the nefarious update, some users still copied and pasted the update URL.

ップには悪意のある不正なアップデートをダウンロードするクリック可能なリンクがついているため、攻撃はこれを利用してユーザーのビットコインを盗むことに成功した。エレクトラムチームは、まずウォレットアプリをアップデートし、リッチHTMLテキスト（図3）を表示できなくなるようにした。それにもかかわらず、複数のユーザーは、加害者によって仕掛けられた罠に陥り続けた。ポップアップに不正なアップデートへの直接リンクが含まれていないにも関わらず、複数のユーザーはアップデートのURLをコピー・ペーストしていたのである。

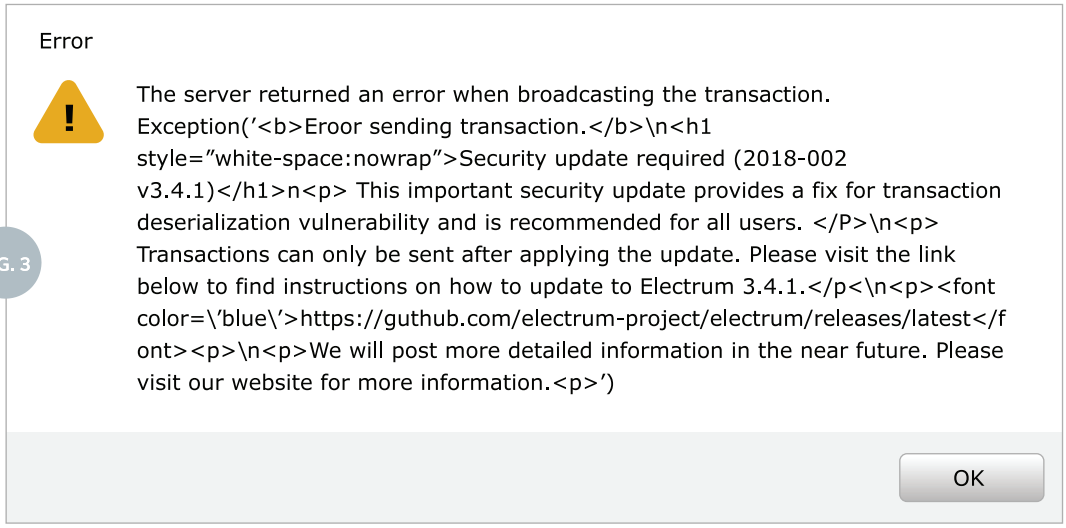


FIG. 3



The Hidden Cost of a Data Breach

In 2018, the Ponemon Institute published a study focused on unraveling the hidden costs of data breaches. This research, sponsored by IBM, showed that the hidden costs that accompany data breaches -- such as reputational damage, time spent on recovery, lost business, etc. -- continue to become costlier year after year.

The study, conducted via interviews with over 2000 IT, protection, and compliance professionals from 477 companies, put the average total cost of a data breach at $3.86 million, representing a 6.4% increase from the prior year. The average cost of data breaches came out to $148 per stolen record, a 4.8% cost increase compared to the previous year.

The research also quantified the cost of “mega breaches”, which are breaches resulting in anywhere between 1 million to 50 million lost records. The estimated total costs for mega breaches range from $40 million to $350 million, usually in proportion to how many records become compromised. Oftentimes, when estimating costs, companies focus on easily quantifiable variables, which leave out more difficult to quantify aspects such as customer turnover, operational costs, etc. In 2017, there were 16 known mega breaches, reflecting a sharp increase from the 9 documented mega breaches of 2013.

The largest contributor to mega breach costs is the loss of business, which is estimated at an average of $118 million for breaches with 50 million records lost. Interestingly, publicly reported costs of many high profile mega breaches fall short of the average reported in the study by Ponemon. This is due to these publicly reported costs often failing to take into account more difficult-to-quantify factors, such as those mentioned at the onstart of this article.

データ侵害の隠れたコスト

2018年、Ponemon Instituteはデータ侵害による隠れコストの解明に焦点を当てた調査を発表した。 IBMが後援したこの調査では、データ侵害に伴う隠れコスト（評判の低下、回復に費やした時間、ビジネスの喪失など）が年々増加することを示唆した。

この調査では、477社の2000人を超えるIT、プロテクション、およびコンプライアンスの専門家とのインタビューを行った。調査の結果、データ侵害の平均総コストは386万ドルで、前年比6.4%の増加となった。データ侵害の平均コストは盗難記録1件あたり148ドルで、前年比4.8%のコスト増となった。

また、この調査では、100万から5,000万件の損失記録となる「メガ侵害」のコストも算定された。メガ侵害の推定総コストは4,000万ドルから3億5千万ドルの範囲で、これは通常は危険にさらされる記録数に比例する。多くの場合、コストを見積もる際に、企業は簡単に数量化できる変数に注目するが、顧客の取引高、運用コストなどの側面を数量化することは困難である。2017年には16件の既知のメガ侵害があり、2013年に実証された9件のメガ侵害からの急激な増加を表わしている。

メガ侵害のコストへの最大の要因は事業の喪失である。事業の喪失は、5,000万件の損失記録侵害に対して平均1億1,800万ドルと推定されている。興味深いことは、多くの注目を浴びたメガ侵害に関して公に報告されたコストが、Ponemon Instituteの研究で報告された平均額を下回っていることだ。この理由としては、この記事の冒頭で述べたように、多くの場合、コストの数量化が困難な要因を計算に入れないことが原因として挙げられる。

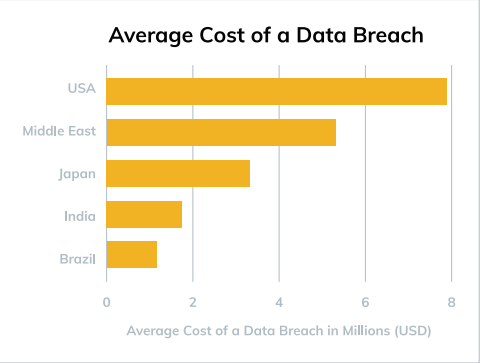
Ponemon Instituteの調査で得られた主な調査結果では、データ侵害における地域と業界の違いについても調べることができた。データ侵害は、米国で最もコストがかかり（平均791万ドル）、続いて中東（平均530万ドル）という結果になっている。データ侵害におけるコストが最も少ない地域は、ブラジル（平均約124万ドル）とインド（平均約177万ドル）だ。日本のデータ侵害の平均コストは、338万ドルと計算されている。

Key findings from the Ponemon study also examined regional and industry differences in data breaches. Data breaches are most costly in the United States (avg. $7.91 million), followed by in the Middle East (avg. $5.31 million). The least costly geographic areas for data breaches are Brazil (avg. $1.24 million) and India (avg. $1.77 million). Japan's average cost of a data breach was calculated to be $3.38 million.

When comparing industries, heavily regulated industries tended to have a higher cost in mitigating the effects of a data breach. Industry costs were compared on a per record basis, with the Health Care sector costing the most at $408 per record, followed by Financial Services at $206 per record.

The study also highlighted factors that decreased breach costs. The greatest impacts on breach costs were related to the amount of time spent containing a breach, as well as investments in technologies that increase response speed. Overall, the average time to identify a breach was 197 days while containing breaches took an average of 69 days. If a company was able to contain a breach in less than 30 days, this saved the company an average of $1 million, compared to companies who took longer than 30 days to contain security breaches. On the other hand, when looking at the numbers from a cost per record perspective, having an incident response team reduced the average cost of a stolen record by $14, while using an AI platform for cybersecurity reduced costs by $8 per stolen record. Ultimately, the best ways to reduce breach costs come down to increasing an organization's ability to recognize and act on a breach quickly.

業界を比較すると、厳格に規制された業界では、データ侵害の影響を軽減し、対処するコストが増加する傾向があった。業界コストは記録ベースで比較され、ヘルスケア部門が記録1件当たり408ドルで最も高く、続いて金融サービス部門で記録1件当たり206ドルという結果になった。



また、この調査では、侵害コストを削減した要因も浮き彫りにした。侵害コストの最大の影響は、侵害を阻止するために費やした時間のほか、対応速度を上げるテクノロジーへの投資に関係していた。全体として、侵害を特定するのにかかる平均日数は197日だったが、侵害を阻止する平均日数は69日だった。セキュリティ侵害を阻止するのに30日以上かかった企業と比較して、30日以内に阻止できた企業は平均100万ドルのコストを節約できた。一方、記録あたりのコストの観点から数字を見ると、サイバーセキュリティにAIプラットフォームを採用した場合、盗難記録1件あたりの平均コストが8ドル削減される一方で、事件ト対応チームを採用した場合は、盗難記録1件あたりの平均コストを14ドル削減した。結果、侵害コストを削減する最善の方法は、侵害を迅速に認識し、対処する組織の能力を向上することにある。

TBT: TRENDS, BREACHES, AND THREATS

Maintaining proper security measures is more than installing antivirus software on devices; it is a dynamic process which requires not only in-depth knowledge of current cyber threats and trends, but also the education of all levels of an organization on proper cyber security practices. In a world where sophisticated hackers often target people with little understanding of computer security, a general lack of cyber security personnel and education within organizations makes it easier for hackers to take advantage of security flaws and gain access to sensitive information.

適切なセキュリティ対策は、デバイスにウイルス対策ソフトウェアをインストールするだけでは維持できない。これは動的プロセスであり、現在のサイバー脅威と動向に関する深い知識だけでなく、適切なサイバーセキュリティプラクティスに関する組織のあらゆるレベルの教育も必要とする。経験豊富なハッカーがコンピュータセキュリティについて認識不足の人々を狙うことが多い中、、セキュリティ専門人材や組織内教育の欠如は、ハッカーの機密情報へのアクセスを簡単に可能にしてしまう。

Emotet: Dissecting a Trojan Horse

For companies and organizations, the cyber security Achilles heel of today, which will remain so for the foreseeable future, is their personnel. 2018 was graced with an increase in incidents related to one particularly unforgiving Trojan malware known as Emotet, which focuses on exploiting this exact vulnerability. Detecting Emotet has proven to be rather difficult due to its highly advanced modular and polymorphic nature. Polymorphic malware is malware that can change itself over time--Emotet can make changes to itself every time it is downloaded, therefore allowing it to more easily evade signature-based detection (detection based on patterns displayed by a malware during previous known cyber attacks).

First launched in 2014, Emotet was originally deployed to attack German banks and steal financial data by intercepting network traffic. Since then, Emotet has been intensely reworked to target a wider and wider pool of industries and organizations. Last year, Emotet made a significant impact in the U.S, causing never-to-be-recovered files, disrupting business arrangements, and denting reputations.

Emotet's infiltration approach

Emotet focuses on Windows-based systems and infiltrates them via highly advanced phishing campaigns disguised as seemingly harmless social approaches. For example, Emotet tricked quite the number of unsuspecting individuals into clicking malware-containing holiday-related emails, which supposedly contained digital holiday greeting cards.

Emotet's phishing emails usually contain a Microsoft Word document as an attachment or via an internet link. These Microsoft Word files are accompanied by

Emotet：トロイの木馬を分析

企業や組織にとってサイバーセキュリティの肝となるところは、今後の課題として残るであろう「人員」である。2018年はEmotetとして知られているトロイの木馬マルウェアが猛威を振るった。Emotetの検出は、高度なモジュラーかつポリモーフィック型の性質を持つことから非常に困難であることが証明されている。また、ポリモーフィック型マルウェアは時間の経過とともに変化する。つまり、Emotetはダウンロードされる度に変化できるため、シグネチャーベースの検出をより簡単に回避することができる。

2014に最初に登場したEmotetは元々、ネットワークトラフィックを傍受してドイツの銀行を攻撃・財務データを盗むために構築されたものである。それ以来、Emotetはより幅広い業界や組織をターゲットにするために徹底的に作り直されてきた。昨年はファイルの復元を不可能にしたり、業務を乱したり、企業の評判を落としたり等、Emotetは米国に重大な影響を与えた。



Emotetの侵入経路

Emotetは、Windowsベースのシステムに焦点を当て、一見無害な社会的アプローチに見せかけた高度なフィッシングキャンペーンを介して侵入する。例えば、電子グリーティングカードを含んでいるように思わせ、マルウェアが含まれているホリデー関連のEメールをそれと疑わない人々がクリックするように仕向けるのである。

Emotetのフィッシングメールには通常、Microsoft Wordファイルが添付もしくはリンクの形で含まれている。Microsoft Wordファイルには、ファイル内で仕組まれたタス

“malicious” macros, which are a series of commands that execute a given task automatically within a file. For security purposes, macros are usually disabled by default in Microsoft Word. Therefore, hackers must find a way to manipulate the recipients of their messages into enabling such macros--hence the elaborate phishing campaigns. When these macros are enabled, they activate PowerShell commands that download the full version of Emotet from previously compromised servers.

クを自動的に実行する一連のコマンドである「悪意のある」マクロが付随しているが、通常セキュリティ上の理由でマクロはデフォルトで無効化されている。そこでハッカーは、フィッシングキャンペーンを作成し、受け取った者がそれを有効化するように仕向けるのである。このマクロが有効化されると、PowerShellコマンドが作動し、すでに侵害されたサーバーからフルバージョンのEmotetがダウンロードされる。

Persistence and propagation

Emotet, once executed on a new device, aims to establish a foothold within the system before then attempting to propagate further and spread to other systems. To do this, Emotet first ensures its automatic and recurrent execution each time a current infected user initiates a system booting or reboot. Emotet accomplishes this by creating scheduled tasks and registry key entries. It will also generate numerous files in the system’s root directories with random generated names that appear legitimate, stashing its payload in storage paths situated off of the AppData/local and AppData/roaming directories, for example.

Once it has established its foothold, Emotet will focus on its propagation. Its first line of action is to collect information on the infiltrated device and operating system, before reporting back to its origination servers, in order to determine what additional malware to download onto the compromised system. These additional downloads usually involve various tools, used to excavate the system to access credentials and other information.

Example Tools Emoted may seek to download onto its victim’s system:

MailPassView: Used to access email account information, such as passwords

持続性と伝播

Emotetは新しいデバイス上で実行されると、そのシステム内に基盤を築き、そこからさらに他のシステムに伝播するように設計されている。これを行うために、Emotetはまず既に感染したユーザーがシステムを起動または再起動するたびに、スケジュールされたタスクとレジストリキーエントリーを作成し、これにより自動実行と繰り返し実行を行うようになっている。また、システムのルートディレクトリに、実際にありそうな名前のファイルを自動生成し、そのペイロードを例えば、AppData/localやAppData/roamingディレクトリの外にあるストレージパスに隠すのである。

基盤が確立されると、Emotetは伝播にフォーカスするようになる。その最初のアクションとして、侵入されたデバイスとオペレーティングシステムに関する情報を収集し、発信サーバーにレポートする前に、侵入先のシステムにどのマルウェアを追加でダウンロードするか特定するのである。これらの追加ダウンロードは通常、多様なツールを利用し、認証情報やその他の情報にアクセスするために実施される。

Emotetが被害者のシステムにダウンロードを試みるツールの例：

MailPassView：GmailやMicrosoft Outlook等、メジャーなEメールクライアントを持つEメールアカウントのパスワード等のアカウント情報にアクセスするために使用される。

and logins, for email accounts with prominent email clients, such as Gmail and Microsoft Outlook, among others.

WebBrowserPassView: Swipes passwords stored with everyday web browsers like Chrome, Firefox, or Safari.

Outlook PST scraper: Scans Outlook messages seeking names and email addresses from the compromised user's Outlook account.

Other Trojans: Depending on the victim, Emotet may seek to download a number of other trojans. For example, when targeting a banking institution, it may download Dridex, IceID, or Zeus Panda, all which can be used to monitor browser activity in order to gain access to user bank account information.

Once these many downloads are complete, Emotet will begin propagating through first attempting to access the user's contact list to collect contact information of people within the user's social network, such as the user's family, friends, work colleagues, clients, etc. Using the user's social media account, Emotet will then deploy new phishing campaigns on the user's social media networks targeting the user's contacts. This gives the phishing attack more legitimacy when sending fraudulent emails, which increases the likelihood of future recipients becoming compromised. Secondly, Emotet will employ brute force guessing to gain access to computers connected to the infected user's network if there are any. If these computers or other machines have poor password protection, Emotet can find an easy way into other computers while bypassing the need to trick a user into giving it access to the new systems.

WebBrowserPassView：Chrome、Firefox、Safari等、日常的に使用されるウェブブラウザ上に保存されているパスワードを盗む。

Outlook PST scraper：Outlookメッセージをスキャンして侵入先のユーザーのOutlookアカウントから名前と電子メールアドレスを探す。

その他のトロイの木馬：被害者によっては、Emotetがその他のトロイの木馬をダウンロードする可能性もある。例えば、金融機関がターゲットになっている場合、Dridex、IceID、Zeus Pandaをダウンロードしてブラウザの動作を監視し、ユーザーの銀行口座情報にアクセスすることに使用される。

これらのダウンロードが完了すると、Emotetはまずユーザの連絡先リストににアクセスし、ユーザーの家族、友人、同僚やクライアント等、ユーザのソーシャルネットワーク内の連絡情報を収集を開始する。そこからユーザーのソーシャルメディアアカウントを使用し、そのユーザーの連絡先をターゲットに詐欺メールを送信することで新たなフィッシングキャンペーンを展開する。この方法では通常のメールに見えるため、これを受け取った人々がさらに被害にあう確率が高くなるのである。また、Emotetは感染したユーザーのネットワークに接続されているコンピューターが存在する場合、それらにアクセスを試みる。これらのコンピューターやその他マシンのパスワード保護が脆弱な場合、ユーザをだましてアクセス情報を収集することもなく簡単にアクセスする方法を見出すことが可能である。



Protecting Against Emotet

Because Emotet often infiltrates organizations by compromising employee devices, more organizations are beginning to adopt a set of guidelines and employee training solutions to manage the Emotet issue. These practices, even though they don't wholly neutralize the Emotet threat, have been known to significantly contain it and similar malware. A few simple guidelines are listed below:

- Keep your systems and virus protection software up-to-date with the latest patches and system updates.

- Educate yourself and your team about phishing, and avoid downloading attachments or clicking unknown links. If you must click on an unknown link, think before you do so, and look for potential abnormalities first.

- Educate yourself and your team on how to create strong passwords. Using two-factor authentication is another good best practice to boost account security.

If you suspect you have been compromised with the Emotet trojan, or if you are looking for a list of technical actions to complete, consult the website of the United States Computer Emergency Readiness Team (US-CERT). US-CERT, which is operated by the US Department of Homeland Security, has a comprehensive profile of Emotet, including a list of recommended actions for both prevention and remedy of Emotet.

Emotetからの保護

Emotetは多くのケースで、従業員のデバイスを経由して組織に侵入するため、この問題への対策として一連のガイドラインと従業員トレーニングを採用する組織が増えている。これらのプラクティスは、Emotetの脅威を完全に無力化するものではないが、Emotetや同様のマルウェアを著しく抑制することで知られている。下記はいくつかの簡素化されたガイドラインである。

- 最新のパッチとシステムアップデートを使用して、システムとウイルス対策ソフトウェアを最新の状態に保つようにする。

- - フィッシングについて自分自身および自分のチームを教育し、添付ファイルのダウンロードや知らないリンクのクリックを避ける。知らないリンクをクリックしなければならない場合、クリックする前にどのようなリスクが生じるか熟考する。

- - 強力なパスワードを作成する方法について自分自身および自分のチームを教育する。 2要素認証（2FA）を使用し、アカウントのセキュリティを高めることも、もう1つの最善な方法である。

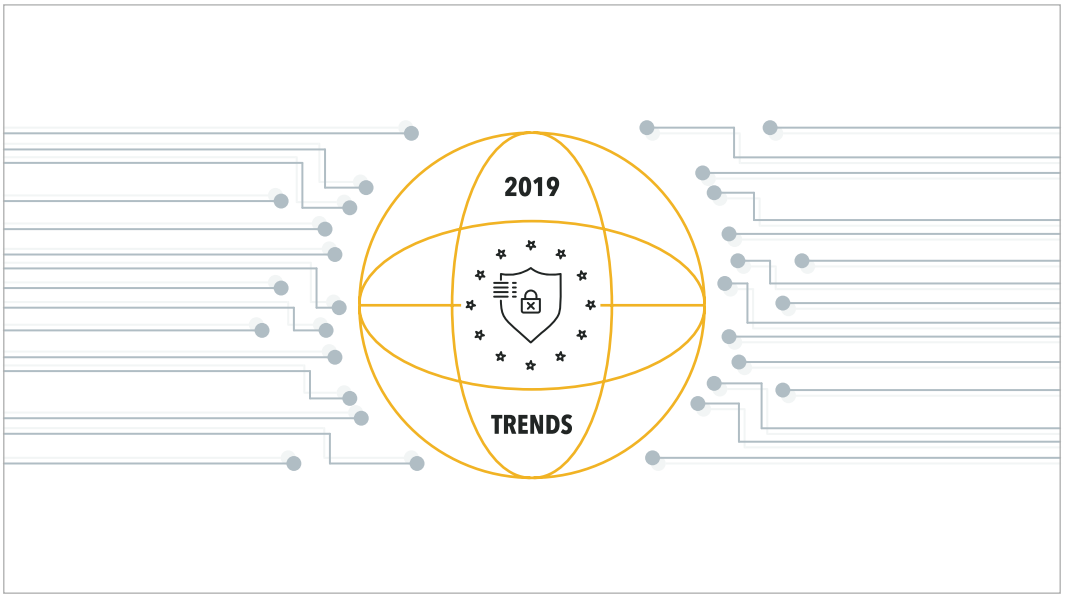
Emotetに感染していると思われる場合、またはEmotetに関する技術的な対策情報を探している場合は、米国コンピュータ緊急対応チーム（US-CERT）のWebサイトを参照するとよい。米国国土安全保障省によって運営されているUS-CERTは、Emotetの予防と対策に関して推奨される行動のリストを含む、Emotetに関する包括的なデータを持っている。

Security Trends for 2019 and Beyond

There is little doubt that the world of cyber security will continue to evolve as hackers find new ways to exploit systems and organizations improve their security in an ever-continuous game of cat and mouse. Here, we elaborate on four security trends that we expect to remain strong throughout 2019.

2019年以降のセキュリティ動向

いたちごっこのように、ハッカーが新しい方法でシステムを悪用する度にサイバーセキュリティの世界が進化していくというのは、ほぼ間違いない。この記事の中で2019年を通して有力な4つのセキュリティ動向について詳しく説明していく。



1 - Security is a people problem:
The biggest flaw in cybersecurity is the ability for hackers to easily exploit people's inexperience with safe computing practices. This is not new, and as discussed in regards to Emotet malware in the previous article, people remain the soft underbelly of organizations seeking to defend against cyber crime. In 2019, as was the case in 2018, the industry will continually experience a shortage of skilled cybersecurity professionals, which, studies have projected, will lead to a 3.5 million personnel deficit by 2021. Therefore, growing the number of people entering the field, and fostering a more diverse talent pool, will become critical to the cyber security industry as it seeks to move forward and avoid the significant expected shortages.

1 - セキュリティは人の問題：
サイバーセキュリティの最大の欠点は、ハッカーが安全なコンピューターの使用方法を熟知していない人々を簡単に悪用できてしまうということである。これは新しい現象ではないが、前回のEmotetマルウェアに関する記事でも説明したように、サイバー犯罪から身を守ろうとしている組織の弱点は「人」なのである。2019年も2018年同様、サイバーセキュリティ業界では継続的に熟練したサイバーセキュリティ専門家が不足することが予測されている。研究では、2021年までに350万人の人的赤字になると見積もられている。従って、この分野に参入する人の数を増やし、より多様な人材を確保することは、サイバーセキュリティ業界が前進し、予想される深刻な人材不足を回避しようと努める中で極めて重要になる。

Organizations will need to search for ways to reduce personal negligence on behalf of employees that increase risk exposure. Educating the workforce and improving employee personal security practices are needed wherever possible. A good place for organizations to begin is to start improving access privilege management practices by ensuring that only individuals who need permission to access various systems, or parts of a system, have that access. Doing this right means periodically reviewing and assessing who has what privileges within a system; in other words, to be successful, it cannot be just a one-and-done exercise, but a continuous effort and ongoing initiative.

組織は、リスクを増大させる従業員に代わって人的過失を少なく方法を模索する必要がある。例えば、従業員の教育および各個人のセキュリティ対策の改善は随時行うことが必要であり、まずはアクセス許可を持つ人間のみが各種システムまたはシステムの一部へアクセスできるようにするといったアクセス権限管理の慣行を改善するところから始めることが最適である。これを正しく行うには、システム内で誰が何の権限を持っているか定期的に確認・評価することが必要となり、言い換えればセキュリティを万全にするためには1回限りの対策ではなく、長期的かつ継続的に取り組んでいくことが必要となる。

2 - Data privacy as an avenue for growth:
Organizations that consider data privacy as an avenue for business success and innovation will place themselves in a position to thrive in the global and digital economy. The rise of data protection laws, as well as continued proliferation of regulation in years to come, are forcing people to think about how they manage data in ways they have never had to worry about before.

2 - 成長の手段としてのデータプライバシー：
データプライバシーを事業の成功と革新の手段であると考慮している組織は、グローバルおよびデジタル経済において伸びていくであろう。データ保護法の進化と規制の継続的な増大により、これまで心配する必要のなかった方法でデータを管理することを考えざるをえなくなってきているからだ。

Managing data and curating it properly is not about avoiding data, but about having the right data components available in just the right amounts and accessible to just the right people at just the right time. Improving data management is not just an opportunity to comply with laws, but also an opportunity to improve management practices, reduce biases, and promote more efficient use of available data.

データを管理し、適切にキュレートすることは、データを回避するという意味ではなく、利用可能な適切なデータコンポーネントを適切な量のみ、適切な人に、適切なタイミングでアクセス可能にすることである。データ管理の改善は、単純に法令を遵守するということではなく、管理プラクティスを改善し、偏りを削減し、利用可能なデータの効率的な使用を促進する良い機会でもある。

3 - Embracing automation:
Automation is continuing to take on a greater role within the security industry, improving all facets of cyber defense. Automation has shown the ability to reduce the mean time to detection when detecting threats and breaches, but also helps reduce negative impact

3 - 自動化を受け入れる：
自動化は、セキュリティ業界内でより大きな役割を担い続けており、サイバー防御のあらゆる面を改善している。実際、自動化により脅威や情報漏洩を検出するまでの平均時間が短縮されていることが証明されている。また、日常的な作業を自動化することで、サイバーセキュリティ業界を悩ませている人的

from the lack of personnel resources plaguing the cyber security industry by automating routine tasks. Solutions that use automation to pull data from different security products and aggregate them into a single and easy-to-read pane, for example, are a great help to detecting, analyzing, and responding to malware more rapidly.

This act of collecting and aggregating data from a variety of sources efficiently has been dubbed SOAR: Security Orchestration, Automation and Response. Not only does leveraging automation reduce the number of tasks that need to be performed by humans, it enables the use and analysis of far more data more quickly than before, which in turn enables security teams to better protect their systems from threats. In the end, automation allows for three high-level strategic advantages: faster detection and action, optimization of scarce resources, and an ability to perform actions the human brain cannot, such as processing and analyzing larger and larger swaths of information in real-time without having to pause for a security analyst to investigate.

4 - Securing data in the public cloud: Another 2018 trend which is expected to continue and thrive in 2019 is the protection of data in the public cloud. In recent times, organizations have realized that the cloud is a crucial enabler of digital transformation. This has paved the way for both faster innovation and improved business agility.

Given the exponential growth of companies seeking to move data to the cloud, cloud security is taking on a greater importance for organizations. Crucial to establishing a secure cloud is understanding that security in the cloud is a partnership between the cloud provider and the organization storing their data in the cloud. Security of the cloud falls to the cloud provider; however, maintaining

資源不足による悪影響を軽減する上でも役立っている。例えば、自動化を使用して様々なセキュリティ製品からデータを取得・集積し、それを単一の見やすいウィンドウに纏めるソリューションは、マルウェアをより迅速に検出、分析、対応する上で非常に役立つ。

様々なソースからデータを効率的に収集して集約することを、SOAR（Security Orchestration（セキュリティオーケストレーション）、Automation（オートメーション）、Response（レスポンス））という。自動化を活用することで、人間が実行するタスク数が減るだけでなく、以前よりも莫大なデータ量の使用と分析が可能になり、セキュリティチームは脅威からのシステム保護を強化できるようになる。まとめれば、自動化は1）より迅速な検出とアクション、2）乏しい資源の最適化、3）一時停止することなく、大量の情報のリアルタイム処理・分析等、人間では不可能な作業をする能力、という3つの高度な戦略的利点をもたらすことが可能である。



4 - パブリッククラウドでデータを保護： 2018年から継続的に盛んになっていくであろうと予想される2019年のもう一つの動向は、パブリッククラウドのデータ保護である。近年、組織はクラウドがデジタル変革の重要な要因であることを認識しており、これによりイノベーションの迅速化とビジネスの機敏性の向上が可能となった。

データをクラウドに移行しようとする企業の急激な増加を考慮すると、クラウドセキュリティは組織にとってますます重要な位置を占めるようになっている。セキュアなクラウドを確立するためには、クラウドのセキュリティとはクラウドのプロバイダーとクラウドにデータを保存する組織間の協力関係が必要であるということを理解する必要がある。クラウドのセキュリティはクラウドプロバイダーにゆだねられているが、クラウド内のセキュリティ管理はそのクラウドプロバイダーを

security in the cloud will often fall to the organization using the cloud provider. As such, the cloud provider presents the security provider with normalized cyber security and data-relevant telemetry feeds, while the organization storing their data is responsible for leveraging that information to monitor and improve security. This enables organizations storing data on the cloud to avoid the hassle of collecting all the security relevant telemetry data, since it is provided by the cloud provider. Instead, organizations storing data in the cloud can focus their resources on analyzing it to ensure their security.

使用する企業に任されていることが多い。よって、クラウドプロバイダーは通常のサイバーセキュリティーとデータ関連のテレメトリーフィードをセキュリティープロバイダーに提供し、データを保存する組織はその情報を活用してセキュリティの監視・改善をしている。組織は、セキュリティ関連のテレメトリーデータは全てクラウドプロバイダーから提供されるため、このデータを収集する手間を省くことができる。この省いた時間でデータ分析に集中することが可能となる。



The OPM Hack: When “Tony Stark” Took on the U.S.A.

In 2015, The United States Office of Personnel Management (OPM); the agency that deals with the affairs of the United States’ government for all civilian federal employees, realized that it had been hacked. Surreptitiously, millions of SF-86 forms, which contained personnel data for persons seeking security clearances from the government, along with millions of recorded fingerprints, were stolen by an entity that has remained unidentified to this day.

The official Congressional report on the incident states that it is unclear how intruders first accessed the OPM systems. However, further investigation successfully mapped how the attackers proceeded once they gained entry.

A first set of hackers first probed OPM networks in 2013. In the congressional reports, these hackers were labeled X1. As of 2013, this first group of hackers was unable to gain access to particularly sensitive data stored by the OPM. However, X1 was able to access manuals as well as information regarding the computer system’s architecture. This security incident did not go unnoticed for long. By March 2014, the OPM became aware that their systems had been breached. In response, the OPM decided to adopt a strategy that was ultimately unsuccessful: they would first let the hackers remain within their systems, and monitor them, in a bid to gain counter-intelligence data. This decision was made under the belief that the hackers would not be able to gain access to sensitive data, such as large swaths of personal information on United States employees.

However, the attacks continued and became more advanced. Once the OPM observed the hackers beginning to deploy hacking tools known as “keyloggers”,

OPMのハッキング：「トニー・スターク」のアメリカ進出

2015年、連邦政府の全連邦職員を対象に米国政府の問題を扱う機関、米国人事管理局（OPM）はハッキングに気付いた。何百万もの記録された指紋と併せて、政府からの機密保護を求めている人の人事データが入ったSF-86フォームがエンティティに盗まれ、現在に至るまでその身元は不明のままだ。

事件に関する公式の議会報告は、ハッカーがOPMシステムにアクセスした方法は不明であると発表している。しかし、調査を進めて、ハッカー侵入後の攻撃方法をマッピングすることに成功した。

2013年に、最初のハッカーの団体がOPMネットワークに探りを入れ始めた。議会報告では、これらのハッカーをX1と呼んだ。2013年の時点では、この最初のハッカー団体はOPMによって保存された特に機密性の高いデータにアクセスすることができなかった。しかし、X1はマニュアルやコンピュータシステムのアーキテクチャに関する情報へのアクセスに成功した。 2014年3月頃には、OPMはシステムの侵害に気付いたが、対応策は効果的ではなかった。つまり、ハッカーをシステム内に留まらせ、カウンターインテリジェンスデータを獲得しようと目論むハッカーを監視するという作戦だったが、これは、ハッカーが政府職員の個人情報といった機密データにアクセスすることは不可能であるという（誤った）確信の下で採用されたのだった。

しかし、ハッカーの攻撃は続き、もっと高度になった。 OPMは、ハッカーがデータベース管理者のワークステーションにキーボード入力時のキー入力を記録する「キーロガー」と呼ばれるハッキングツールを導入し始めたことを確認したとき、OPMは今こそハッカーをシステムから追い出す時だと判断した。ユーザーがパスコードを入力した時に、キーロガーがそれを習得する可能性を恐れたのである。データベース管理者のパスコードが危険にさらされる危険性が高まったため、システムをリセットすればハッカーをシステムから一掃できると考え、OPMはシステムリセットを実行した。 OPMのアプローチは狙い通

which record keystroke inputs when people type into a keyboard, the OPM decided it was time to boot the hackers from the system fearing the keyloggers could be used to learn database administrator passcodes as users typed them. With the increased risk of compromising database administrator passcodes, the OPM executed a system reset believing the system reset would purge the attackers from their systems. The OPM's approach worked, and the hacking group referred to as X1 was expelled from the system.

However, the OPM's confidence in their ability to have ridden themselves of the assailants was misplaced. Another attacking group, dubbed X2 in the congressional report, which may or may not have been working in tandem with X1, had previously established a secondary foothold within OPM's systems. X2 created a backdoor in the OPM's systems for later entry. They were able to do this by stealing credentials from a government contractor known as KeyPoint. KeyPoint was one of two contractors working on behalf of the OPM to help conduct background checks and had been given access to OPM servers. By October 2014, X2 had succeeded in delving through the department's interior server where employee records were kept. This resulted in over 4.2 million employees' records being stolen in addition to large quantities of fingerprint data stored by the OPM.

Despite how X1, the initial group of hackers, first gained access to the OPM's network remaining uncertain, it is significant to point out that the OPM had previously been criticized for its poor security management practices. It also remains unclear whether or not groups X1 and X2 were the same group or were working in tandem. However, the original information stolen by X1 would have been very helpful to X2.

りとなり、X1と呼ばれるハッキング団体はシステムから追い出された。

しかし、ハッカー団体を撃退したというOPMの確信は見当違いだった。X1と連携して働いていたことが疑われるX2と呼ばれるもう1つのハッカー団体が、既にOPMのシステム内に第2の基盤を確立していた。 X2は後の侵入に向けてOPMのシステムに裏口を作成していた。X2は、KeyPointとして知られる政府の請負業者から資格情報を盗んでそれを実現できたのだ。KeyPointは、OPMに代わってバックグラウンドチェックを行う業者の1つで、OPMサーバーへのアクセス権を与えられていた。 2014年10月までに、X2は従業員の記録が保管されている部門の内部サーバーを調べることに成功した。その結果、OPMに保存された420万人を超える従業員の記録だけでなく、大量の指紋データも盗まれたのだった。
最初のハッカー団体であるX1がOPMのネットワークへのアクセス権を獲得した方法はあやふやなままだ。ただ重要なことは、OPMが以前からセキュリティ管理の不備を理由に批判されていたことである。また、グループX1とX2が同じ団体であったか、あるいは連携して作業していたかについても不明なままだ。しかし、X1によって盗まれた元の情報はX2にとって非常に有益な情報だった。

こういったハッカー攻撃から明らかなように、OPMのシステムセキュリティはかなり疑わしいものであった。それ以上に、ここでもまた、最も脆弱なセキュリティ上の欠陥は人的ミスと自信過剰であった。X1の侵入にもかかわらず、OPMはセキュリティプラクティスを迅速に見直して適応させなかった。それどころか、X1排除を目的としてシステムリブートを最初に実行した時に、実際にハッカーを撃退したか否かもきちんと確認しなかった。

2015年4月、OPMのネットワーク上で暗号化トラフィックを調査していたエンジニアが、何者かのOPMシステムへの侵入を感知したことで、X2の存在に気づいた。このエンジニアは、OPMのシステムインフラストラクチャ上で、opmsecurity.orgが造り出したウェブサイトに接続される、mcutill.dllと

The OPM's system security, as evidenced by these attacks, was rather questionable. Beyond that, here, once again, the most flagrant security flaws at display were human error and overconfidence. Despite the initial breach, the OPM did not rapidly overhaul and adapt their security practices. Instead, they made assumptions around whether or not they had actually ridden themselves of the hackers when they executed a first system reboot to expel X1.

X2 was first noticed in April 2015, when an engineer inspecting encrypted traffic on OPM's networks noticed that someone had probed the OPM's system. He noticed a system file named mcutill.dll on OPM's system infrastructure, which connected to a website coined opmsecurity.org. The component, mcutill.dll, looked similar to a component that is part of the McAfee security software suite, a software protection suite that OPM did not use. Furthermore, opmsecurity.org was not a domain name that belonged to the OPM agency.

This website was determined to be a tool for hackers to gain access to the OPM servers. Hidden beneath the mcutil.dll was a malware offshoot of a malware known as PlugX, while the opmsecurity.org domain was being used by the hackers as a server through which they could send commands to the OPM systems. The domain name was registered to fake aliases, notably Marvel's Iron Man "Tony Stark" and Captain America "Steve Rogers".

Based on general consensus, the OPM was likely hacked by state-sponsored hackers working for the Chinese government. Some of the tools and methods used during the attack have previously been associated with the Chinese government. For example, the PlugX variant has previously been seen in

いう名のシステムファイルがあることを発見したのだ。このmcutill.dllは、OPMが使用していないMcAfeeセキュリティソフトウェアスイートの一部のコンポーネントに似ていた。しかも、opmsecurity.orgはOPM機関が保有するドメイン名ではなかった。

このWebサイトは、ハッカーがOPMサーバーにアクセスするためのツールであると判明した。 mcutil.dllの下に隠されていたのはPlugXとして知られているマルウェアの派生物だった。opmsecurity.orgドメインはハッカーがOPMシステムにコマンドを送信するサーバーとして使用されていた。ドメイン名は、偽名のエイリアスとして、Marvelのアイアンマン「トニー・スターク」そして、キャプテン・アメリカ「スティーブ・ロジャース」が登録されていた。

一般的なコンセンサスから、OPMはおそらく中国政府に雇われた国家後援のハッカーによってハッキングされたものと考えられる。攻撃に使用された一部のツールや方法は、以前中国政府との関係が認められたものだった。例えば、PlugXの変種は、以前は香港やチベットの政治活動家に対する攻撃で見られた。2018年9月、米国の国家安全保障担当顧問を務めるジョン・ボルトン氏は、中国が確かにOPMのデータ漏洩の背後にあると述べた。

個人情報が盗まれた個人の被害を減らすために、米国政府は2025年までにこの漏洩の影響を受けたすべての人に無料の与信監視およびID保護サービスを提供することを決定した。与信監視サービスを含む米国政府の被害総額は、最大で合計10億ドルに達する可能性がある。しかし、最も懸念されることは、このハッキングに関する最新ニュースの不足だ。これまでのところ、盗まれたデータが使用されているという兆候はほとんどない。



attacks against political activists in Hong Kong and Tibet. In September 2018, John Bolton, the acting US National Security Advisor, cited that China was, indeed, behind the OPM Data Breaches.

In a bid to decrease the potential for damaging effects to individual persons whose identities were stolen, the US government opted to provide free credit monitoring and ID protection services to all who had been affected by the breach through 2025. Total costs of the breach to the US government, including credit monitoring services, could reach as much $1 billion in total. However, what may be the most concerning is the lack of recent news about the hack. Thus far, there has been little indication that the stolen data is being used.



TAKING ACTION

In the cyber security world, staying apprised of existing vulnerabilities, and adapting to them quickly, is crucial. From understanding how to protect open source code, to learning how to build an organization that is truly resilient to cyber threats, organizations must stay vigilant and continually educate themselves on the security flaws that can be exploited by hackers. The following section conducts detailed explorations of two different topics in cyber security: securing open source code and fostering more secure human behavior. It is our hope that the information presented will help illustrate and guide organizations on how to take concrete action to improve their security moving forward.

サイバーセキュリティの世界では、既存の脆弱性を常に把握し、迅速に適応することが重要である。オープンソースコードの保護方法から、サイバー脅威に対して真に回復力のある組織の構築方法まで、組織は常に警戒心を持ち、ハッカーに悪用される可能性を排除するよう絶えず学ばなければならない。次のセクションでは、サイバーセキュリティにおいて2つの異なるトピック、オープンソースコードの保護とより安全な人々の行動の促進について詳しく説明する。ここで提示された情報が、組織がセキュリティ向上に向けて具体的な措置を取ることに役立てば幸いである。

Securing Open Source Code

Open source components play an increasingly central role in the development of software worldwide. These essential building pillars provide developers with multiple “off-the-shelf” possibilities when assembling their products, and are expected to play an increasingly important role in the development of future applications. Software company Synopsys’ audit group Black Duck, which focuses on open source security management and compliance, conducted an audit of 1,100 plus commercial codebases in 2017 and found that the average open source composition of the analyzed codebases had increased from 36% to 57% over a period of one year.

Despite this considerable use of and dependence on open source code, the software industry has shown laxity in ensuring that open source components always meet expected security standards. Black Duck’s audit revealed that more than 75% of the examined applications had a minimum of 1 vulnerability within their codebase, while the average number of vulnerabilities in each application across the entire group of 1,100 plus examined codebases was 64. This neglect for open source software security is often said to be caused by the underestimation of the level of usage that these components undergo. Another reason attributed to this laxity is the nature of open source susceptibilities and the difference in addressing such vulnerabilities compared to when addressing security flaws in proprietary software. In a recent survey of over 5000 IT professionals by Sonatype, another company focused on helping developers expedite their software development when using open source code, researchers found a 71 percent increase in open

オープンソースコードの保護

オープンソースコンポネント（OSC）は、世界的なソフトウェアの開発の中心的役割を担っている。OSCは、開発者が製品を組み立てる際に即使用できるオプションを提供し、将来のアプリケーションの開発においてますます重要な役割を果たすことが期待されている。オープンソースのセキュリティ管理およびコンプライアンスに焦点を当てているソフトウェア会社Synopsysの監査グループBlack Duckは、2017年に1,100以上の商用コードベースの監査を実施している。分析されたコードベースの平均オープンソース構成は、一年間で36%から57%までに増加した。



OSCの幅広い使用と依存にもかかわらず、ソフトウェア業界は、オープンソースコンポネントが常に期待されるセキュリティ標準を満たしていると錯覚して来た。Black Duckの監査では、1,100以上の調査済みコードベースのグループ全体で各アプリケーションの平均脆弱性数は64なのに対し、調査対象のアプリケーションの75%以上がコードベース内に1つ以上の脆弱性が、あった。オープンソースソフトウェアのセキュリティに対するこの放置状態は、コンポネントの使用レベルの過小評価によって引き起こされていると一般的に言われている。この放置状態に起因するもう1つの理由は、オープンソースの脆弱性の性質と私有ソフトウェアのセキュリティ上の欠陥を対処する場合と比較した場合の脆弱性への取り組みの違いだ。Sonatypeによる5000人以上のIT専門家の最近の調査では、オープンソースコードを使用する際、開発者がソフトウェア開発を促進するのを

source code related breaches over the past 5 years. As these breaches continue to increase, and especially as high profile breaches related to open source vulnerabilities occur such as the Equifax hack in 2017, organizations are starting to focus greater attention on the potential for vulnerabilities within the open source components they use.

Addressing Open Source Code Safety
A significant issue of concern with the usage of open source code is that it is readily available for exploitation since it is openly available to the public. The approximation of the quality and security of the code is another issue of worry, as there is difficulty in establishing if the code was properly reviewed or not. However, supporters of open source software argue that because it is available for review by an entire community, it is easier to ensure quality. The reasoning is that making the code available to more people for review will lead to more errors or vulnerabilities being caught.

Despite the sound logic to this argument, this idea has faced skepticism in recent years, especially with the discovery of the Heartbleed and Shellshock vulnerabilities. The Heartbleed vulnerability affected the OpenSSL cryptography library, while the Shellshock bug was a series of bugs in the Unix bash shell. Both Heartbleed and Shellshock vulnerabilities were only noticed years after the affected code was released.

The glaring reality is that open source projects have experienced exponential growth along with their increased usage. As a result, there is a lot more code to be reviewed, but not necessarily a proportional growth in reviewers. A large part of why open source components are used so widely is because they lower costs and make development more efficient. As such, the incentives to use open source components don't

助けることに焦点を合わること、過去5年間で、オープンソースコード関連の侵害が71%の増加したことが明らかになった。有名な2017年のEquifaxハックをはじめとする侵害が増えるたび、、組織は使用するオープンソースコンポーネント内の脆弱性の可能性にさらに焦点を当てるようになった。

オープンソースコードの安全性への取り組み
OSC使用に関する最大の懸念は、OSCは誰もが利用可能なため、悪用されやすいことだ。コードの品質とセキュリティの品定めが困難なのもは、もう1つの問題点である。というのはは、コードがレビューがされたかどうかの見極めるのは簡単ではないからだ。しかし、オープンソースソフトウェアの支持者は、オープンソースコードがコミュニティ全体でレビューが可能であるため、品質確保が容易であると主張している。この理論は、多くの人々がコードを利用し、レビューできるようにすることで、より多くのエラーや脆弱性が見つかるということだ。

このような根拠ある論理にもかかわらず、HeartbleedやShellshockの脆弱性の発見に伴い、この考えは近年疑問視されている。 Heartbleedの脆弱性はOpenSSL暗号ライブラリに影響を及ぼし、一方でShellshockのバグはUnixのbashシェルの一連のバグであった。しかし、 HeartbleedとShellshock両方の脆弱性は、影響を受けたコードのリリース後数年たってやっと発見されたのだった。

オープンソースプロジェクトは、使用量の増加と共に、急速な成長を遂げている。このため、レビューすべきコードはよく多く存在するが、必ずしもレビュー担当者が比例して増加するわけではない。 OSCがこれほど広く使用されているのは、OSCの使用が、コスト削減や、より効率的な開発に貢献するためである。 そのため、OSCを使用するインセンティブは、必ずしもコードのレビューと改善へのインセンティブを意味するわけではない。よって、OSCを使用している多くの開発者は、ソースコードのレビューしないままOSCをダウンロードしているだけだ。かとい

necessarily also incentivize reviewing and improving the code. Therefore, many of the developers using open source components are only downloading the open source code without reviewing the source code itself. That said, open source code exploitation is rarely done through unknown vulnerabilities. Rather, it is carried out through previously documented vulnerabilities that are publicly available, just like the code itself is. These known vulnerabilities are made available to enable development teams to do the necessary fixes to secure their applications. The downside of this is that hackers also follow these publications and exploit them to their benefit.

Finding Flaws in Open Source Code

Open source components are not subjected to the traditional application security testing methodologies that proprietary software uses. The reason is not far-fetched; open source depends on a widespread network of contributors which each add their own work to the code. Hence, a different approach, which allows dependence on communities by managers of open source projects to uncover vulnerabilities and start fixes, is needed.

Usually, contributors, ethical hackers, and researchers from the open source community check the code via the deployment of automated and manual tools to uncover vulnerabilities. This process is slow and onerous; nevertheless, it yields results. When a vulnerability is uncovered, the open source project managers are contacted by the contributor who has discovered the bug. This is because the project manager or managers are the formal owner or owners of the code. Thus, they are responsible for the bugs. From there, usually the managers will report the flaw to the MITRE Corporation, a non-profit organization backed by the U.S. government; other times, however, the

って、未知の脆弱性を介してOSCの悪用が行われることはほとんどない。むしろ、まさにコードその物のように、既に公になっている脆弱性を介して実行される。これらの既知の脆弱性は、開発チームがアプリケーション保護のための必要な修正ができるように、利用できるようになっている。だがそれは、ハッカーも公開された内容を確認し、自身の利益のために内容を不当に利用できることも意味している。



Official Logo for Heartbleed

オープンソースコードの欠陥を発見

オープンソースコンポネントは、私有ソフトウェアが使用する従来のアプリケーションセキュリティテスト手順の対象外である。その理由は想像に難くない。オープンソースは、それぞれが自分自身の作業をコードに追加する貢献者の広範囲なネットワークに依存しているからだ。従って、オープンソースプロジェクトの管理者が脆弱性を発見して修正を開始するという、コミュニティ主導アプローチが必要である。

通常、オープンソースコミュニティの貢献者、倫理的なハッカー、および研究者は、脆弱性を検出する自動および手動ツールの展開を通じてコードを確認する。このプロセスは時間がかかり、面倒な作業だが、結果を生む。脆弱性が発見されると、オープンソースプロジェクトの管理者は欠陥を発見した貢献者から連絡を受ける。これは、プロジェクトの管理者が、コードの正式な所有者であるからだ。このように、プロジェクトの管理者が欠陥の責任を負う。その後、通常は管理者がその欠陥を米国政府が支援する非営利団体MITREコーポレーションに報告する。その他の場合は、管理者がプロジェクトの問題追跡システムにセキュリティ上の欠陥に関する情報を提供するか、欠陥に関する勧告を別の形で行う。

managers will instead provide information on the security flaw in their project issue tracker or make some other form of advisory about the flaw.

If the open source managers contact MITRE, MITRE will assign the open source software vulnerability a unique ID for tracking purposes. These IDs are maintained in a Common Vulnerabilities and Exposure, or CVE, database. For instance, the initial ID for the Shellshock vulnerability was CVE-2014-6271; this includes the year when the report occurred followed by an assigned number.

To give managers the necessary time to fix a reported bug but still encourage rapid reporting of issues, the exact details of a discovered bug will not be immediately published. Instead, only the affected components can be seen publicly until MITRE can confirm the vulnerability in addition to a 2 to 3 month grace period granted to the affected code managers. At the end of the 2 to 3 month period, details about the vulnerability are published and the flaw will then be listed in the National Vulnerability Database (NVD) along with an impact score. The National Vulnerability Database is a U.S. government repository that includes databases of security references and security-related software flaws. Once vulnerability details are listed online, companies will race to patch their systems before hackers can take advantage of the newfound vulnerability.

However, not all vulnerabilities are reported to MITRE's CVE database. In some cases, open source project managers who discover a vulnerability may decide to publish it on alternate security advisories, or just simply add it to their project issue tracker. In instances like these, vulnerabilities do not appear in the National Vulnerability Database (NVD), as they do not receive a CVE number. Due to the lack of uniform reporting

オープンソースの管理者がMITERに連絡した場合、MITERはオープンソースソフトウェアの脆弱性を追跡するために固有のIDを割り当てる。これらのIDは共通脆弱性識別子（CVE）データベースで維持されている。例えば、Shellshockの脆弱性の初期IDはCVE-2014-6271で、この初期IDには、報告された年とその後に割り当てられた番号が入っている。



Official Logo for Shellshock

検出された欠陥を迅速に報告することを推奨しているが、報告された欠陥の修正に必要な時間を管理者に与えられるために、検出された欠陥の正確な詳細はすぐには一般に公表されない。代わりに、MITREがこの脆弱性を確認できるまでは影響を受けたコンポネントだけが一般公開され、かつ影響を受けたコード管理者に2〜3か月の猶予期間が与えられ、る。 2〜3ヶ月の猶予期間後に、脆弱性に関する詳細が一般に公表され、その後、脆弱性がインパクトスコアと共にNational Vulnerability Database (NVD)にリストアップされる。NVDは、セキュリティ関連のデータベースやセキュリティ関連のソフトウェア欠陥のデータベースを含む米国政府のリポジトリだ。脆弱性の詳細がオンラインでリストアップされると、ハッカーが新たに発見される脆弱性を利用する前に、企業はシステムを修正しようと急ぐ。

しかし、すべての脆弱性がMITREの共通脆弱性識別子CVEデータベースに報告されているわけではない。脆弱性を検出したオープンソースのプロジェクトの管理者が別のセキュリティ勧告に公開するか、単にプロジェクトの問題追跡システムに追加するだけという決定をする場合もある。このような場合、脆弱性はCVE番号を割り当てられないため、NVDには表示されない。脆弱性に関する報告が統一されておらず、脆弱性を列挙している幅広い情報源があるため、すべてのオープンソースの脆弱性に関する適切

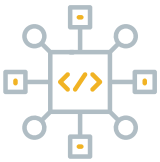
practices and the range of sources where reported vulnerabilities may be listed, it can become quite strenuous to compile relevant details on all open source vulnerabilities. As a result, open source code users risk missing out on critical vulnerabilities while nefarious actors may have already discovered them. To mitigate that risk, it is best to stay up to date by keeping an eye on as many sources of information as possible. Although some sources other than the CVE and NVD repositories are privately run databases that charge for access, such as VulnDB which is administered by Risk Based Security, many are free such as Linux Security, Node Security Platform (NSP), RubySec, and any open source component GitHub Issue Trackers. Some of these databases focus on specific coding languages, which can help narrow down which sources are best. Linux Security is the most significant vulnerability database related to Linux components, while the Node Security Platform, or NSP, makes provision of security information in Node.js modules and NPM dependencies. RubySec offers security resources and information dedicated to the Ruby community.

Fixing Open Software Flaws

Addressing vulnerabilities in open source code is entirely different from fixing flaws in proprietary code. In the case of proprietary code, once developers detect a potential security flaw, those who are responsible for the creation of the code are responsible for the research and validation required to perform the necessary code fixes. However, this is often not the case with open source vulnerabilities.

Usually, when open source components are pulled from a repository by a developer, they are often taken as they are. This means that developers integrate the open source components without gaining an in-depth familiarity with the code before hand. While this works well as long as the code is functional, this

な詳細をまとめることは骨の折れる仕事になる。その結果、OSCのユーザーは重大な脆弱性を見逃す危険性があり、悪意のあるハッカーがむしろそれらを既に発見している可能性がある。このリスクを軽減するには、できるだけ多くの情報源に目を通すことが最善である。CVEとNVDリポジトリ以外では、RIsk Based Security所有のVulnDBのように、の個人運営されており、データベーススへのアクセスが有料なものもあるが、Linux Security、Node Securiyt Platform (NSP) 、RubySec、GitHub Issue Trackerなどは無料でアクセス可能である。 これらのデータベースの中には、特定のコーディング言語に焦点を当てているものもあり、。どのソースが最適であるかを絞り込む場合に有益だ。例えば、 Linuxセキュリティは、Linuxコンポーネントに関連する最も重要な脆弱性データベースである一方、Node Security Platform (NSP) は、Node.jsモジュールおよびNPM依存関係のセキュリティ情報を提供する。 Ruby-Secは、Rubyコミュニティ専用のセキュリティリソースと情報を提供している。



オープンソフトウェアの欠陥を修正

オープンソースコードの脆弱性への対処は、私有コードの欠陥の修正とはまったく異なる。私有コードの場合、開発者が潜在的なセキュリティ上の欠陥を発見すると、コード作成担当者がコード修正を実行するために必要な調査と検証を担当する。しかし、これはオープンソースの脆弱性にはあまり当てはまらない。

通常、オープンソースコンポネントが開発者によってリポジトリから移動させられても、変更されたオープンソースコンポネントは、そのままとされることが多い。つまり、開発者は事前にコードを熟知していなくても、オープンソースコンポネントを統合することができるということだ。これは、コードが機能している限りうまく動作するが、問題が起きた際には、開発者はオープンソースプロジェクトの貢献者に一層頼ることにもなる。従っ

setup also makes the developer more reliant on open source project contributors when an issue is exposed. The challenge posed by this adoption of open source components, therefore, is that software developers must come up with fixes that do not affect their end product, which may not always be possible for more interdependent code, especially when the developers in question lack familiarity with the open source code or the aspects of the code that are vulnerable.

Fortunately for developers, a majority of vulnerabilities listed in the CVE database have at least one potential fix listed. Similarly to the information on vulnerabilities, information on remediation can be distributed among many repositories or issue trackers. This can sometimes make figuring out the open source community's recommendations difficult for security and development teams, similarly to how finding vulnerabilities in the first place can become challenging due to the widespread reporting practices across multiple sources. Despite these challenges, and regardless of whether or not developers have clear fixes available to them or not, they have multiple options for recourse when addressing vulnerabilities. Options range from applying a fix directly to the specific functionality where a vulnerability is located, to removing the entire open source component as a whole. Ultimately, developers seek to apply the fix that has the most minimal impact on the broader functionality of their project, often making an applied fix to the affected component much more appealing than removing it entirely.

As the use of open source components in applications has continued to increase in recent times, so, too, has the number of newly discovered vulnerabilities which developers must address.

て、このオープンソースコンポネント採用時の課題とは、開発社が最終製品に影響を与えないコードの修正方法を考え出さなければならないということだ。特に、ソフトウェア開発者がオープンソースコードや脆弱なコードの側面に精通していない場合には、より相互に依存するコードでは、必ずしも可能ではないかも知れない。



開発者にとって幸運なことに、CVEデータベースにリスト化されている大多数の脆弱性には、潜在的な修正が少なくとも1つ併記されている。脆弱性に関する情報と同様に、修復に関する情報は、多くのリポジトリまたは問題追跡システムに拡散することができる。複数の情報源の中の広範な報告慣行により、初期段階で脆弱性を発見することが困難になり得るのと同様に、セキュリティや開発チームがオープンソースコミュニティの勧告の理解を困難にすることがある。これらの課題、そして開発者が使える明確な修正案の有無に関係なく、開発者は脆弱性に対処する複数の方法がある。その方法は、脆弱性が存在する特定の機能に直接修正を適用することから、オープンソースコンポーネントを全体として削除するまで幅広いが、 最終的には、開発者はプロジェクトの機能全体への影響が最も少ない修正を適用しようとする。

アプリケーションにおけるオープンソースコンポネントの使用頻度が近年増加しているため、開発者が取り組まなければならない新たな脆弱性の発見も増えている。

この困難なタスクを処理するため、開発者はこの急速に増加する脆弱性に優先順位を付ける新しく改善された方法を模索しなければならない。例えば、CVSSスコアの点で最もランクが高い脆弱性は、最も差し迫っている脅威と見なされる。しかし、チームがある複数の問題に対処するためには、いくつか

In a bid to handle this difficult task, developers must seek new and improved ways to prioritize vulnerabilities among this rapidly increasing number of issues. For example, vulnerabilities ranked highest in terms of their CVSS scores are obviously considered most pressing. However, other factors should also be considered when prioritizing a team's plan of attack to address a given flaw or set of flaws. Before taking CVSS scores into consideration, one must first deal with the highest-impact issues that can ensure the greatest security of the product.

Because open source components are reusable and are customarily fashioned for a variety of different customers and use cases, they contain many functionalities. As a result, a developer's application may only take advantage of a portion of the overall functionalities available within an open source component.

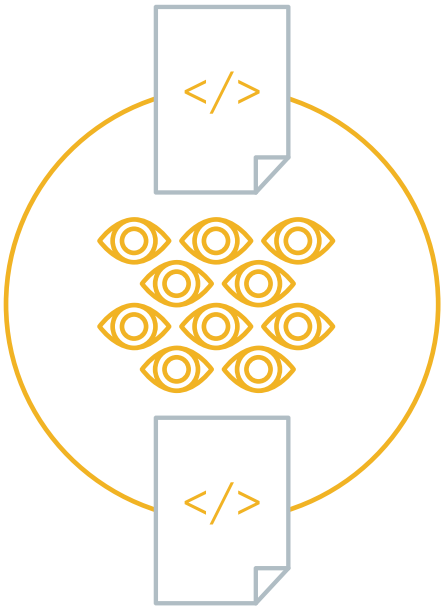
Developers' prioritization of the fixing of software vulnerabilities hinges on the developers' ability to ascertain which functionalities are being used and if unused functionalities can still affect the application's security. Being capable of prioritizing vulnerabilities can help developers focus on critical issues that demand the most attention. This prioritization not only improves the security of applications, but also helps boost engagement and cooperation from developers by enabling them to maximize their impact and make more meaningful contributions to a product.

Another key step to fixing open source security flaws is inculcating security awareness and testing throughout the software development process and before an open source component is used. Seeking to test software earlier on during the development process to uncover flaws before the software release is often referred to as "shifting left". The "shift left" concept came about from the growing

の要素を鑑みて優先順位をつける必要がある。 CVSSスコアを考慮に入れる前に、製品のセキュリティを最大に確保することができる最も影響力がある問題に最初に取り組まなければならない。

OSCは再利用可能であり、さまざまな顧客や使用状況に応じて作られているため、多くの機能が含まれている。そのため、開発者のアプリケーションは、各オープンソースコンポネント内で利用可能な全体的な機能のほんの一部しか活用しない可能性がある。

ソフトウェアの脆弱性に対し、どの修正を優先するかどうかは、開発者自身の、OSCのどの機能が使用されているか、および未使用の機能がアプリケーションのセキュリティに影響を与える可能性があるかを確認する能力次第だ。脆弱性に優先順位を付けることは、開発者が最も注意を要する重大な問題に集中するのに役立つ。この優先順位付けは、アプリケーションのセキュリティを向上させるだけでなく、開発者による影響を最大化し、製品へ一層意味のある貢献をすることで、開発者の関与と協力を促進させることが可能だ。



オープンソースのセキュリティ上の欠陥を修正するもう1つの重要なステップは、OSC使用前に、ソフトウェア開発プロセス全体にセキュリティの認識とテストを実施することである。ソフトウェアのリリース前に、開発プロ

difficulty of speeding up the development process without compromising the quality of each new software release. By incorporating software security testing earlier on in the delivery roadmap in addition to general functionality testing, issues are often detected earlier by development teams when it is quicker, easier, and less costly to fix security issues. The concept actually gets its name from shifting testing “leftward” along the software creation and delivery timeline.

Previously, “shift left” testing focused only on software functionality testing; however, it has expanded to include security applications over the past several years. Open source security is a natural candidate to ‘shift left’ because the information on its vulnerabilities is publically available. This means developers have the opportunity to search and understand the potential vulnerabilities of an open source component before they decide to deploy it. That said, even with this leftward shift, developers should remain vigilant and ready for newer bugs that may not come to light until after the open source code is already being used. A clear example of failure to do this is demonstrated by how Black Duck’s audit revealed that 4% of codebases included in the audit had yet to address the Heartbleed vulnerability, despite it having been a full 4 years since the vulnerability was disclosed in addition to being a well known, high profile vulnerability that had received a lot of publicity.

セスの早い段階で欠陥を発見するためにソフトウェアのテストをすることは、「シフト・レフト」と呼ばれる。「シフト・レフト」の概念は、新しいソフトウェアの開発を品質を落とさないままスピードアップすることの困難さから生まれた。一般的な機能テストに加え、開発の早い段階でソフトウェアのセキュリティテストを取り入れることで、開発チームは問題を早期に検出でき、セキュリティ問題より迅速、容易、低コストで修正できる。この概念は、ソフトウェアの開発スケジュールに沿ってテストを「左に」シフトすることから来ている。

従来、「シフト・レフト」はソフトウェアの機能テストだけに焦点を当てていた。しかし、ここ数年でセキュリティアプリケーションを含むテストに拡張されている。オープンソースセキュリティは、脆弱性に関する情報が一般に公開されているため、「シフト・レフト」がごく自然に選ばれる。つまり、開発者は、OSCの展開を決める前に、潜在的な脆弱性を見つけて理解するチャンスがあるということだ。とは言っても、「シフト・レフト」をした後も、開発者はOSC使われるまでは明らかにならない新しいバグの可能性に警戒しておくである。これが失敗した明らかな例としてHeartbleedが挙げられる。このケースでは、脆弱性が判明して多くの注目を集めて4年が経過したあとも、脆弱性に対しまだ対処していないことをBlack Duckの監査が明らかにしている。

In Conclusion

As technology continues to advance, and software plays an ever increasingly crucial role in modern life, developers will continue to rely on open source components in application development in order to keep up with the present day demand to make our high-tech devices work faster, smarter, and better. It is up to organizations deploying open source software to ensure such software is used securely. If hackers' targeting of various software applications in recent years is any indication, their attacks on applications are only going to increase. Indeed, software applications remain easy targets if left defenseless. The open source components which we use to create our applications must therefore be fortified by excellent software vulnerability detection and repair. Companies and other organizations must therefore both innovatively embrace open source components as well as adopt the correct tools, mindset, and best practices that enable them to operate these components in a responsible manner.

結論

テクノロジーが進歩し続け、ソフトウェアも現代生活においてますます重要な役割を果たすようになるにつれ、開発者は現在のハイテク機器をより迅速に、スマートに、向上させるため、アプリケーション開発でOSCに頼り続けるだろう。そのようなソフトウェアを確実にしっかりと使用できるかは、オープンソースソフトウェアを展開する組織次第である。近年、ハッカーはさまざまなソフトウェアアプリケーションを標的にする兆しを見せており、アプリケーションに対する攻撃は増加する一方だ。実際、ソフトウェアアプリケーションは、無防備のままであればハッカーの簡単な標的になる。従って、アプリケーション作成に使用するオープンソースコンポネントは、優れたソフトウェアの脆弱性の検出と修復によって強化されなければならない。そのため、企業や他の組織は、オープンソースコンポネントを革新的に取り入れ、責任ある方法でこれらのコンポネントを操作するための正しいツール、考え方、およびベストプラクティスを採用する必要がある。





Becoming a High-Reliability Organization for Cybersecurity

The human challenge in cyber security arguably poses one of the most significant threats in the cybersecurity landscape today. More and more, hackers are targeting people, not simply technologies. A company can possess the most high-tech information technology infrastructure available on the market, but without proper email hygiene and cybersecurity training for employees at all levels of an organization, the company becomes vulnerable to cybercrime. According to Inc., business email compromise constitutes nearly half of the approximately $1.5 billion in total losses due to internet crime. Business email compromise occurs when human employees click on links in emails from unknown senders, and can result in the payment of thousands of dollars to hackers by unknowing cybercrime victims.

Other forms of cybercrime targeting humans can be waged via email, social media, the internet, cloud-based applications, or other means. They can be waged by individual hackers seeking financial gain, or by another country's government to protect their national interests.

How can people help ensure better cybersecurity? Employees should be trained to identify cybercrime attacks. Training humans to detect malicious email or internet activity can go a long way, but threat detection and response can also be bolstered by automated tools. That said, individual people and automation are not enough, organizational structure and culture as a whole is pivotal.

The Human Factor in Cyber Security: A High-Reliability Organization Problem

The human problem in cyber security is an example of a High Reliability Organization, or HRO, problem. HROs are

サイバーセキュリティにおいて高信頼性組織（HRO）になる

サイバーセキュリティにおける人的課題は、今日のサイバーセキュリティの展望における最も重大な脅威のひとつだ。ハッカーは単に技術ではなく、ますます人々を標的にしている。企業は市場で入手可能な最もハイテクな情報技術インフラを保有することができる。しかし適切な電子メールの衛生状態と、組織のあらゆるレベルの従業員に対するサイバーセキュリティトレーニングが確保できなければ、組織はサイバー犯罪に対して脆弱になる。 Inc.(月刊誌)によると、ビジネス上の電子メールの侵害は、インターネット犯罪による被害総額（約15億ドル）のほぼ半分を占めている。従業員が知らない人間から送られたメールに含まれるリンクをクリックすると、ビジネス上の電子メールが侵害され、未知のサイバー犯罪の被害によって、ハッカーへ数千ドルの支払いが発生する可能性がある。

人々を標的にした他の形態のサイバー犯罪は、電子メール、ソーシャルメディア、インターネット、クラウドベースのアプリケーション、またはその他の方法を介して行われる可能性がある。金銭的利益を求めている個々のハッカー、あるいは国益を保護したい他国の政府によって遂行されているのだ。

どうすれば向上したサイバーセキュリティを確保できるだろうか？答えは、従業員が、サイバー犯罪攻撃を特定できるようにトレーニングを受けることでがある。悪意ある電子メールやインターネット活動を検出するように人々をトレーニングすることに加え、自動化ツールによって脅威の検出と対応も強化することも役に立つ。そうであっても、個人へのトレーニングと自動化ツールだけでは十分ではなく、全体としての組織構造と教養が極めて重要だ。

サイバーセキュリティにおける人的要因：高信頼性組織（HRO）の問題

サイバーセキュリティにおける人的課題は、高信頼性組織（HRO）の問題がひとつの例として挙げられる。HROは、長期間にわた

a type of organization that must maintain a high level of safety for long periods of time. HROs have a high level of risk and complexity which makes the avoidance of accidents a high priority to operate error-free and avoid catastrophic failure. Example of HROs include air traffic control systems, nuclear propulsion vessels, and electric power grids among others. While cyber crime often does not have the same immediate and visible affect that say, an airplane crash or a nuclear accident will have, the systemic effects can be just as costly and devastating.

Although some cyber attacks are more visible in their impact, because they may cause a problem with systems on a wide scale, other cyber attacks are more subtle. Cyber attacks can go unnoticed for years until, for example, a foreign country builds the same technology another country has due to years of intellectual property theft through undetected cyberattacks. The Wall Street Journal recently reported that the U.S. Navy and its industry partners are the target of cyber attack by hackers based in China who have successfully stolen national security secrets from the U.S. military over the past several years. In one breach, a Navy contractor involved in the building of a secret high-tech naval missile to be used with U.S. military submarines was hacked. In this China attributed cyber attack, the secret plans for this naval missile were stolen.

The human factor problem in cybersecurity is analogous to the big catastrophe problem found in HROs. While there is often not an immediate or visible impact in cybersecurity, the long-term effects are the same, if not worse. For example, while it may not seem disastrous or urgent to protect United States cybersecurity because there are no visible impacts such as a nuclear meltdown or accident, the theft of secret plans for the construction of

る高度な安全性を維持する必要がある組織のタイプだ。HROにはハイレベルのリスクと複雑さがあるため、エラーのない操作と壊滅的な失敗を招かないよう、事故の回避が最優先事項となる。HROの例として、航空交通管制システム、原子力推進船、および電力網が挙げられる。多くの場合、サイバー犯罪は、航空機墜落事故や原子力事故のように直接的で目に見える影響を与えないが、組織的な影響は、航空機や原子力事故と同様に費用がかかり、壊滅的になる可能性がある。

一部のサイバー攻撃は、広範囲に渡ってシステムに問題を引き起こすことがあるために、影響がより明白だ。しかし、その他のサイバー攻撃は手口がもっと巧妙である。何年間も気付かれないままのサイバー攻撃も存在する。例えば、ある国が別の国と同じ技術を構築するために未検出のサイバー攻撃をして、知的財産の盗難が長年に渡る時だ。ウォール・ストリート・ジャーナル紙は最近、米海軍とその産業パートナーが、サイバー攻撃の標的であると報告した。このハッカーたちは、中国を拠点とし、過去数年間にわたって米軍から国家安全保障上の機密を盗み出したことに成功した。ある侵害では、米軍潜水艦と使用される機密のハイテク海軍ミサイルの製作に関与していた米海軍の請負業者がハッキングされた。中国が関係するサイバー攻撃により、この海軍ミサイルの機密計画が盗まれた。

サイバーセキュリティにおける人的課題は、HROに見られる大きな問題と類似している。つまり、短期的あるいは可視的な影響が出ることは少ないが、長期的な効果は同じようなものである。例えば、核のメルトダウンのような可視的な影響がない以上、合衆国政府のサイバーセキュリティ保護は、緊急を要するように見えないのかも知れない。しかし、海軍ミサイル建設機密計画の盗難は重大な問題であり、さらに米国が世界における軍事的優位を失うきっかけになる可能性がある。もうひとつ例を挙げれば、2017年に信用調査機関を標的にしたEquifaxのハッキングは、史上最高額の損益を与えた事件となった。Equifaxは米国国土安全保障省の指示通り、必要なセキュリティパッチの

a naval missile could be a significant liability and even cause the U.S. to lose their global military supremacy. Another example of a vulnerability resulting in significant damages is the Equifax hack which targeted the credit reporting bureau in 2017 and is the most costly hack in corporate history. Equifax failed to install required security patches as directed by the U.S. Department of Homeland Security, which left hackers able to easily break into the system and query the credit monitoring company's servers over 9,000 times. According to a report by the U.S. House of Representatives Oversight Committee, this hack, which exposed the sensitive personal information of nearly 150 million users, was "entirely preventable."

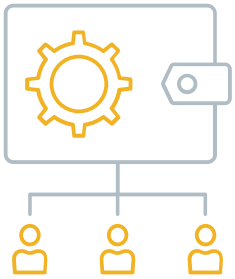
HROs exist to mitigate and reduce risk when there is an incredibly thin margin of human error. In the next section, we'll dive into what HROs are and why they are so critically important to avoid disasters in complex, high-risk enterprises.

What are the characteristics of High-Reliability Organizations (HROs)?
High-Reliability Organizations, or HROs, are organizations which operate by special principles due to the fact that their daily operations require a high level of safety to ensure that no catastrophic accidents occur. Risk minimization in HROs occurs by prioritizing safety, performance, and shared goals; developing a culture of reliability and safety, trial-and-error learning, and redundancy beyond technology – such as dependable human intervention -- to ensure that the critical needs of the organization are met.

What are the characteristics of HROs and how are they used to tackle complex problems? Because serious problems and accidents can be highly dangerous in HROs, they enable the diagnosis of organization reliability states and ways to improve the functioning of the

インストールを出来なかったため、ハッカーがシステムに侵入し、クレジット監視会社のサーバーに9,000回以上クエリを実行した。米国下院監督委員会の報告によると、およそ1億5000万人のユーザーの機密情報が盗まれたこのハッキングは「完全に防止することができた」ものであった。

HROは人的ミスの可能性がほぼ無い時に、リスクを軽減するために存在する。次のセクションでは、HROとは何か、複雑でリスクの高い組織の災害を回避するためにHROが極めて重要である理由について説明する。



高信頼性組織（HRO）の特徴とは？
高信頼性組織（HRO）は、HROは、日常業務に致命的な事故を発生させないために高いレベルの安全性を必要とするため、特殊な原則に従って運営される。安全性、パフォーマンス、および共有の目標を優先することで、HROのリスクは最小化させる。つまり、組織の重要なニーズを確実に満たすために、信頼性、安全性、試行錯誤による学習、テクノロジーを超えた冗長性の教養を構築するのだ。（例：信頼できる人間の介入など）

HROの特徴とは？ HROは複雑な問題への取り組みにどのように利用されているのだろうか？ HROでは、重大な問題や事故は非常にリスクのあるものになる可能性があるため、組織の信用状態および組織の機能改善方法を診断する。HROで開発され強化された具体的な特性には、監査や問題の予測を通じたリスクの最小化と評価が他の戦略にまして挙げられる。HROは、回復力へのコミットメント、公正な文化、および問題が発生した場合やリスクを軽減する決定が必要な場合の専門的意見の受け入れを勧める。

organization. Specific qualities developed and strengthened in HROs include risk minimization and assessment through audits and problem anticipation, among other strategies. HROs encourage a commitment to resilience, a just culture, and deferring to expertise when a problem arises or decisions need to be made to mitigate risk.

Researchers of HROs are interested in learning how safety can be created and maintained in these complicated systems. Interestingly, HROs are driven not by the absence of negatives, such as a nuclear disaster or cyberattack, but by the presence of positive factors and how to create, maintain, and discuss these positive activities which can help reduce risk.

One example of an HRO is a military aircraft carrier. Such carriers often have many planes taking off in a short period of time, as well as dynamically changing conditions as the carrier travels around bodies of water, and a hierarchy of people who are tasked with ensuring the safe operations of the carrier. All people working on the aircraft carrier, at all levels of work, must work together to make the proper adjustments to ensure that the aircraft carrier can operate safely and fulfill its mission. All staff on the aircraft carrier are: preoccupied with failure and thinking about how to reduce this possibility; understanding of the fact that operations are complex and dynamic; trained to think about the “big picture” and how the carrier’s current state can help support safety; deferent to expertise; and committed to resilience, responding quickly to any safety threats to ensure continued safe operations.

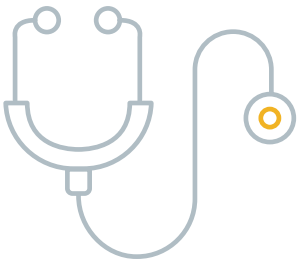
HRO concepts are also applied in aviation and nuclear power industries, firefighting, and the oil and gas industry.

HROの研究者たちは、これらの複雑なシステムでどのように安全性を作り出し、維持することができるかを学ぼうとしている。興味深いことに、HROは、原発事故やサイバー攻撃をはじめとするネガティブな要素の欠如によってではなく、ポジティブな要素の存在、およびリスクを軽減可能なポジティブ活動の作成、維持、話し合いの方法によって動かされる。

HROのひとつの例として軍用航空母艦が挙げられる。このような航空母艦は、短期間で多数の航空機が離陸することが多く、移動時には周囲の環境が著しく変化する。また、確実に航空母艦の安全な運航をするため、担当者間には階級制度がある。航空母艦で勤務する全職員は、あらゆるレベルの業務で、航空母艦が安全に運航し、任務を果たすことを保証するため、全員で力を合わせて適切な調整をするよう動かなければならない。そこで、航空母艦の全職員には以下の特徴が見られる。航空母艦の職員は、失敗する可能性を減らす方法について常に考えている。操作が複雑でダイナミックであることを理解している。航空母艦の「全体像」および航空母艦の現状が安全性のサポートにどのように繋がるか考えるように訓練を受けている。また、専門知識を備えている。そして、航空母艦の継続的な安全運用を確保するために、あらゆる安全上の脅威に迅速に対応して回復することを重視している。

HROの概念は、航空、原子力、消防、石油およびガス産業でも適用されている。ごく最近では、ヘルスケアの管理と提供に関連する複雑な問題に対処するために、ヘルスケア業界でもHROの原理を導入している。医師たちは「まず、害を与えないことをする」ように訓練される。これは、患者へのリスクを減らし、可能な限りベストな医療成果を達成するための複雑な構造の必要性を強調しているのだ。実際、ヘルスケアシステムの失敗は、裨益者にとって悲惨な結果を招く可能性がある。だからHROはヘルスケア企業にとって有益な原理なのだ。医療研究品質局は、高い信頼性を「組織内での持続的なマインドフルネスの条件」と定義している。安全性は、HROにとって常に最優先事項だ。

More recently, the healthcare industry is also adopting the HRO philosophy to deal with the complex issues related to managing and providing health care. Doctors are trained to “first, do no harm,” which underscores the need for complex structures which can be utilized to reduce risk to patients and achieve the best possible medical outcomes. Indeed, HRO is a useful philosophy for health care companies because the consequences of a failure in the healthcare system can be disastrous for the individuals requiring care. The Agency for Healthcare Research and Quality defines high reliability as “a condition of persistent mindfulness within an organization.” Safety is continually prioritized at the top of the list for HROs.





How can HROs be applied to cybersecurity?

The best example of the application of HRO principles to cybersecurity can be found within the U.S. military’s cyber operations. Using an approach borrowed from Admiral Hyman Rickover, the “Father of the Nuclear Navy,” the Pentagon sought to adopt protocols that can help the military personnel avoid mistakes and correct vulnerabilities and anomalies before they magnify and cause significant problems. Just as a nuclear vessel must continually be monitored in redundant ways to ensure the best possible operations, the military’s cyber infrastructure must also be fortified. The military has achieved this, according to the HRO philosophy, using a combination of excellent information technology practices, a highly cyber-aware workforce, and a system which responds rapidly to breaches and vulnerabilities to avoid the theft of sensitive data that could threaten U.S. national security. In 2009, the U.S. Department of Defense’s cyber operations were comprised of several thousands of small network enclaves which did not have the same standards. Recognizing a need for greater unification

HROはどのようにサイバーセキュリティに適用できるか？

サイバーセキュリティに対するHROの原則の適用に関する最良の例として、米軍のサイバーオペレーションが挙げられる。ペンタゴンは、「原子力海軍の父」である海軍大将Hyman Rickoverのアプローチを借用し、軍人のミスを避け、重大な問題を引き起こされる前に、脆弱性や異常の修正を促進するプロトコルを採用しようと試みた。可能な限りベストな操業を確保するためには、原子力潜水艦が継続的、反復的に監視されるべきであるようにに、軍のサイバーインフラストラクチャも強化されなければならない。HROの原理に従い、優れた情報技術慣行、サイバー意識の高い労働力、そして侵害や脆弱性に迅速に対応して米国国民を脅かす恐れのある機密データの盗難を回避するシステムの組み合わせを実行することで、米軍はこれを達成してきた。2009年時点の米国国防総省のサイバーオペレーションは、同じ基準を持たない数千の小規模ネットワーク集団で構成されていた。当時の国防長官Robert Gatesは、ネットワークにおける統一性と一貫性の向上の必要性を認識して、米国サイバー司令部を設立した。米国サイバー司令部では、アメリカ軍のネットワークの厳格な選良の発展のために、HROの概念をうまく適用した。現在、自動化されたツールは、異常を検出し、その異常の脅威レベルを

and coherence in the network, the then-secretary of Defense, Robert Gates, established the U.S. Cyber Command. At the U.S. Cyber Command, HRO concepts were applied successfully to develop a tightly-run crew of elite guardians of the U.S. military's network. Automated tools can now detect anomalies and determine the threat level of said anomalies, and rapidly deploy a fast response in order to prevent cyberattacks from taking hold on the military's servers. These days, thanks to a combination of a highly skilled cyber-savvy workforce and high-tech automated security tools, an estimated 41 million scans, probes, and attacks are monitored and addressed by the Pentagon each month.

The key to the success of the military's Cyber Command is an emphasis on the human side of cybertechnology. As Admiral Mike Rogers has noted, developing a culture of safety, and ensuring that the organization is manned, trained, and equipped with sound operational concepts, is paramount. Without an emphasis on the human factors involved in cyber technology, the U.S. military would not be as successful in fending off rogue and malicious cyber activity on their servers.

Key Characteristics of Cybersecurity HROs

The military's ability to adapt and respond to cyber vulnerabilities is perhaps the best example of a cybersecurity-based HRO. What types of traits are required in an HRO to achieve success of operations on a consistent, day-to-day basis?

Firstly, deviations must be detected immediately and addressed. In the military's cyberinfrastructure, this is accomplished through a mix of human monitoring and automated tools. When a deviation is indeed detected, human operators must work quickly to correct

判断する。そして迅速な対応を展開して、サイバー攻撃が軍のサーバーに侵入するのを防いでいる。今日では、経験豊富なサイバー専門家とハイテクな自動セキュリティツールの組み合わせによって、毎月推定4,100万件のスキャン、プローブ、および攻撃がペンタゴンによって監視および対処されている。

軍のサイバー司令部の成功の鍵は、サイバーテクノロジーの人間的側面に重点を置くことだ。米国家安全保障局取締役Mike Rogersが指摘したように、安全性の教養の構築、組織の訓練、および健全な運用概念を確保することが最も重要である。サイバーテクノロジーに関わる人的要因に重点を置かなければ、米軍は、悪意のあるサイバー活動を米軍のサーバー上でから完全に撃退することはできないだろう。



サイバーセキュリティのHROの主な特徴

サイバー脆弱性に適応し対応する米軍の能力は、おそらくサイバーセキュリティベースのHROの中で最高の模範だ。それでは、HROが一貫して日々の業務に成功するためには、どの類の習性が必要だろうか？

まず、異常をただちに検出して対処する必要がある。軍のサイバーインフラストラクチャでは、人間による監視と自動化されたツールを組み合わせてそれを実現させている。異常が検出された場合、最悪な結果を招く前に、人間のオペレータは迅速に問題解決に取り組まなければならない。HROは専門知識を優先し、専門知識に従う。そのため、適切な専門家に問題が通知され、迅速に対応する

the problem before it become disastrous. HROs prioritize and defer to expertise, so the relevant experts must be notified and work quickly. This means that time is of the essence, so the decision-making process in HROs is somewhat decentralized. This means that individuals who are lower-ranking are tasked with authority decisions in order to maintain a culture of reliability and enable fast response to hazards.

Redundancy of manpower has also proved essential for the U.S. military in terms of protecting their cybersecurity resources. For example, control and information systems must have several decision makers which can arrive at the best possible solution, rather than relying on a single mind which could be susceptible to error. The basic principle here is a simple one familiar to most people – that "two heads work better than one" – that is, many people working together can solve a problem faster and better than one person working alone. The U.S. military has sought to maximize their human resources, recognizing that human error can be the most significant stumbling block to high reliability, by ensuring redundancy in the system.
A third important characteristic of cybersecurity HROs is the prioritization of safety, performance, and the organization's shared goals. This aspect is very human-focused as it requires the close collaboration of all members of the cybersecurity organization in order to enforce the organization's mission and goals to prevent accidents. As Admiral Mike Rogers has stated, this prioritization hinges on the careful development of such an organization, down to the selection of its individual members. This concept crucial to HROs is borrowed from Admiral Hyman Rickover's careful and successful operation of nuclear naval vessels. Admiral Rickover personally interviewed every member of the vessel's crew in order

必要がある。つまり、時間が最も重要であるということだ。よって、HROの意思決定プロセスはある程度分散されている。これは、信頼性の修練を維持し、危険に対して素早い対応を可能にするために、下位の個人にも決定権限が任されていることを意味する。

米軍にとって、サイバーセキュリティのリソースを保護するという点で、人員の冗長性も不可欠であることが証明されている。例えば、制御および情報システムには、エラーの影響を受けやすい1人の意思決定者の考え方に頼るのではなく、最善の解決策を導き出すために複数の意思決定者が必要となる。ここでの基本的な原則は、ほとんどの人にとって馴染みのあるものだ。その原則とは、「三人寄れば文殊の知恵」を指す。1人で作業するよりも、複数人で作業する方が問題をより早くより良く解決できる。米軍は、システムの冗長性を確保することにより、人的ミスが高い信頼性を妨げる最も重大な障害となる可能性があることを認識し、これまで人的資源の最大化を図ってきた。



そして、サイバーセキュリティHROでの重要な特徴の三つ目は、安全性、パフォーマンス、および組織の共有目標の優先けだ。この側面は、極めて人間中心的となっている。事故を防ぐという組織目標と使命を達成するには、サイバーセキュリティ組織のすべてのメンバーの緊密な協力を必要とするからである。 米国家安全保障局取締役Mike Rogersが示したように、この優先事項は、個々のメンバーの採用をはじめとするHROの慎重な構築にかかっている。HROにとって重要なこの概念は、海軍大将Hyman Rickoverによる慎重で、成功した原子力潜水艦の操業から借用したものだ。 Rickoverは、海軍の乗組員全員が組織の任務と目標に適

to ensure that they would be a good fit for the organization's mission and goals and would be able to fulfill the complex duties of the HRO.

The Bottom Line

At the turn of the 21st century, the internet was a new tool and presented enormous global promise. However, in 2019, the increasingly sophisticated nature of the internet, as well as the advent of apps and the internet of things have resulted in an information superhighway that is both more connected and more vulnerable to hacks than ever before. Countries frequently wage cyber war against each other to obtain sensitive details and undermine national security, and therefore, the cyber world represents the newest front lines of battle. Applying the principles of HROs to cyber security can help organizations maintain the highest standards of cyber security and ensure a culture of excellence and resilience, not only mitigating the cyber attack risks but saving their companies valuable time, money, and resources.

任であること、そしてHROの複雑な任務を果たすことができることを確実にするために、全員と個別で面談を行った。

最後に

21世紀の頭には、インターネットは世界的に大きな期待が寄せられた新しいツールであった。しかし、2019年には、インターネットがますます洗練されるほか、アプリの登場やインターネットのサービスにより、これまで以上にインターネットの接続性が向上した。その結果、ハッキングの被害を受けやすくもなった。各国は、機密情報を入手するために、サイバー戦争を頻繁に繰り広げており、国家の安全を蝕んでいる。そのため、サイバーワールドは、最新の戦線となっている。サイバーセキュリティにHROの原則を適用することで、組織はサイバーセキュリティの最高水準を維持する。そして、サイバー攻撃のリスクを軽減するだけでなく、貴重な時間、資金、およびリソースを守れるだけでなく、高い卓越性と回復性を確保できる。

CONCLUDING REMARKS

Xenon specializes in the acquisition, operation, and development of early and mid-stage Software as a Service (SaaS) businesses. Xenon's experienced team recognizes the need to develop strong cyber security standards in our increasingly internet-powered and interconnected world. Therefore, Xenon's products are built with security as a foremost priority.

With a clear lack of cyber security expertise readily available in the market today and the growing impact of cyber crime, Xenon felt the need to help promote cyber security know-how and spread the word in the technology and business communities through its cyber security advisory arm.

Our team is comprised of Certified Information Systems Security Professional (CISSP) certified professionals with both doctorates in Computer Science and master degrees in Cyber Security. If you have any thoughts, comments, or inquiries about this magazine, please join the conversation by contacting us at cybersecurity@xenon.io or visiting us at www.xenon.io/cybersecurity.

Xenonは買収、運用、およびサービス(SaaS)事業として早期・中期段階のソフトウエアの開発に特化している。Xenonの経験豊富なチームは、ますますインターネットに力を与えられて相互につながった世界において、強固なサイバーセキュリティ基準の開発の必要性があることを認識している。

今日の市場では、利用できるサイバーセキュリティの専門知識が明らかに不足している。増え続けるサイバー犯罪の影響の中、Xenonのサイバーセキュリティ顧問がサイバーセキュリティのノウハウを促進し、テクノロジー・事業コミュニティにおいて知識を広げる必要性を感じた。

当社のチームは、情報セキュリティ・プロフェッショナル認証資格(CISSP)の資格を持つ、コンピューターサイエンスの博士号とサイバーセキュリティの修士号の両方を取得した専門家で構成されています。本誌に関するご意見、コメント、ご質問等ございましたらcybersecurity@xenon.ioまでご連絡いただいくか、www.xenon.io/cybersecurityまでご訪問ください。

