Bloomberg Tax

Daily Tax Report®

INSIGHT: Save Money While Fighting Cyberattacks



By Yair Holtzman, Melissa Cohen, and Alex Okin

Given over 50 percent of American adults have experienced a cybersecurity attack, experts can be sure this issue is not going away. The best way businesses can fend off hackers is through investment in emerging technologies to solve current and future security problems. By failing to do so, companies put themselves at risk of losing significant worth. The Research and Development tax credit is a U.S. business incentive offered to companies that experiment with emerging technologies, including cybersecurity solutions. The article offers guidance related to this section of the tax code and highlights the types of core business activities that can qualify for this generous credit.

The Need for Cybersecurity

The threat of cyberattacks are an extreme danger to our society. Cyberattacks have the ability to cause a crippling impact to our lives and the economy at large. With the increased use of technology, there is a corresponding increase in hacker attacks. Hackers have proven their ability to get away with theft of trade secrets, bank money, and cryptocurrency. Beyond financial incentive hackers may attack computer systems to gain political advantage, to advance a social cause, or simply to overcome the intellectual challenge. As IT systems transition to the cloud and devices become more interconnected through the Internet of Things (IoT), these systems will experience an increased vulnerability to being hacked. Small and large companies that harbor valuable and sensitive data are increasingly being targeted by hackers. As a result, there is an increased need for cybersecurity innovation to keep data safe and within its owner's control.

Cybersecurity by definition includes software and protocols designed to protect information systems against disruption or misdirection of services. It also includes protection from harm potentially caused by unauthorized network access and theft of electronic data.

Symantec, the maker behind Norton, found that hackers are enjoying abundant benefits by stealing from individual victims. 689 million people in 21 countries have been victims of cyberattacks, costing an estimated $126 billion in damage in 2016. The U.S. is the greatest target for cyber terror, given 39 percent of Americans age 18 to 65 have experienced some form of cyberattack in 2016. In 2017, more than half of the American adult online community have been targeted by cyberattacks. Unfortunately, these numbers are likely to increase as society continues technological advancements.

Individuals tend to ignore cyber threats by failing to heed warnings and by straying from security protocols. The 2017 Norton Cyber Security Insights Report discovered 970 million people in 20 countries were affected by cybercrimes in 2017. The report found that 58 percent of cybercrime victims admitted to using the same password across all accounts opposed to 17 percent of non-cybercrime victims who use the same password across all online accounts.

The Ponemon Institute uncovered in 2016 that any business has a 26 percent chance of experiencing a data hack when it has more than 10,000 sets of personal data. This is said to cost, on average, $4 million per business. Computer hackers are projected to cost the global economy $6 trillion annually in the next few years. These attacks will attempt to manipulate data, steal money or cryptocurrency, and damage the core business, productivity, and reputation of companies and individuals. However, the true impact of these hacks

 ISSN 0092-6884

could be far worse given the world has never experienced this level of interconnectivity.

Companies must invest in emerging technologies to solve current and future security problems or risk losing significant assets. An example of significant loss of assets is the 2013 Yahoo data breach. This breach was one of the largest data attacks in history affecting over 3 billion user accounts. This cyber-crime involved forfeiture of data including names, email information, telephone numbers, and dates of birth of over 500 million users. The cyberattack caused Yahoo's market valuation to decline by as much as $350 million.

In 2014, eBay, the online auction site, reported a cyberattack revealing the names, addresses, and secret passwords of each of its 145 million users. The hackers reportedly entered eBay's network using the login information of three eBay employees and gained unimpeded access to the user database for a whopping 229 days. Since financial data was kept in a separate database owned by its subsidiary, PayPal, eBay was forced to ask those customers to change their passwords as a precaution.

Most recently, in 2017 credit reporting giant Equifax was hacked. Equifax surrendered personal information like Social Security numbers, addresses, drivers' license numbers, and birth dates to hackers. In total, 145.5 million consumers were impacted and 209,000 consumers had their credit card information stolen.

Cybersecurity software to protect data and systems is constantly being developed due to the ongoing threat of hackers. For example, when a developer creates an algorithm to reverse and prevent new malicious software, there is a reciprocal response from the hacker community. Hackers continuously develop improved malware to attack and penetrate the most recent and advanced cybersecurity solutions and patches.

Integrating cybersecurity software into programs, applications, and devices is absolutely necessary in combatting cyberattack risks. The best way to stay ahead is by innovating through research and development (R&D). However, designing cybersecurity software is a costly endeavor. Companies spend an average 5.6 percent of their overall IT budget on IT security and risk management. As of 2018, Microsoft spent over $1 billion a year on cybersecurity.

The purpose of this article is to help cybersecurity industry executives and decision makers gain a better understanding of the federal R&D tax credit incentive and how it may help their companies overcome the costs associated with developing these innovations. This article also explores the most common cybersecurity solutions and how the federal R&D tax credit incentive may be able to save businesses money when implementing them.

Cybersecurity Technology

Hardware Authentication. Hardware authentication is a security system that uses hardware mechanisms to grant user access. The hardware authenticator serves as a security verifier like a smart card or a USB stick. It is critical for IoT devices. Hardware authentication controls a network of interconnected technologies, which must safeguard its own infrastructure by preventing unwanted devices from connecting to the network.

Bank ATM Machines utilize hardware authenticators to process the ATM Card. An ATM is usually composed of multiple hardware components such as the CPU, magnetic or chip card reader, and a PIN number. The hardware identifier must validate a magnetic ATM card and individual PIN numbers to gain access to ATM services.

The private sector responded to cyber threats by developing software for systems security that would modify and enhance hardware authentication. For example, the Intel 8th Generation Core vPro processor encompasses enhanced hardware security that works to protect system data. In fact, the eighth generation processor is entirely devoted to secure authentication. The Core VPro Processor is a complex authentication solution that can validate identities through facial recognition and minimize the risk of a malicious code by locking firmware when the software is running.

Cloud Technology. Cloud computing is the distribution of computing services over the Internet ''the cloud.'' Many businesses and government units have widely accepted the cloud for data storage purposes and cybersecurity solutions. Features like virtualized intrusion detection, prevention systems, virtualized firewalls, and virtualized systems security are now being utilized on the cloud. Corporate entities have been focusing on data center security by using infrastructure services (IaaS).

Cloud computing is an economical and flexible option for companies seeking cyber security. It allows companies to purchase cloud computing security resources based on the size of the product. Services such as Amazon Web Services (AWS) provides additional cloud computing security by offering solutions on a large scale and provides independent third party audit reports to attest to their internal procedures.

Deep Learning. Deep learning is a subfield of machine learning based on learning data representations like a sound or a picture. Deep learning was first used by social media and marketing companies to learn user information to sell products or services. Cybersecurity companies have been able to use the same technology through malware detection and network intrusion detection. Deep learning systems can prevent a potential attack without any human intervention. This involves artificial intelligence (AI) and machine learning by imitating the way the human brain processes data by monitoring irregular activity. Deep learning examines threats at the entity level instead of the user level. With recent developments in these technologies, cybersecurity specialists can scrutinize business entities comprehensively. Businesses and governments can now use Deep learning to identify cyber threats, learn how they operate, and create advanced autonomous processes for extinguishing the malware.

Cybersecurity Tax Incentives

Rapid evolution in the industry forces companies to constantly innovate or risk falling behind their competition and potentially even being made obsolete. Building better security functionality is more necessary than ever with the threat of cyberattacks. When companies are in the innovation process for developing cybersecurity solutions, companies frequently encounter technical challenges. Some of these challenges include determining the appropriate requirements and design, allow-

ing for efficient integration with other applications, and code complexity that causes multiple points of failure in the cybersecurity software. Addressing and overcoming these issues is critical to the success of the cybersecurity solution and for the success of the business at large. However, these efforts are often time consuming and expensive. Fortunately, the federal government as well as certain state and local governments provide economic incentives to counter and help companies overcome such technical uncertainties and risks undertaken.

The federal research and development (R&D) tax credit was first introduced by Congress in 1981. The purpose of the credit is to reward U.S. companies for increasing spending on research and development within the U.S. On Dec. 18, 2015, President Obama signed into law The Protecting Americans from Tax Hikes Act of 2015 (PATH Act). This legislation retroactively renewed and made the R&D tax credit permanent. Subsequently, on Dec. 22, 2017, President Trump signed into law the Tax Cuts and Jobs Act (TCJA) of 2017, preserving the R&D tax credit. This was the only significant remaining business tax credit in the tax code.

Many employers' activities associated with business initiatives undertaken in cybersecurity will qualify for the federal R&D tax credit. As such, the R&D tax credit is available to businesses that uncover new, improved, or technologically advanced cybersecurity products, processes, principles, methodologies, or materials. In addition to ''revolutionary'' activities, in some cases, the credit may be available if the company has performed ''evolutionary'' activities such as investing time, money, and resources toward improving cybersecurity products and processes. Correctly calculating the R&D tax credit is critical—for maximizing the taxpayer benefit, which will ultimately lower the taxpayer's effective tax rate and potentially generate cash flow, and for achieving sustainability in case of IRS examination. Importantly, the ultimate success of a cybersecurity project is not required in order to qualify for and claim these incentives, since employee activities related to cybersecurity projects that ultimately fail are equally rewarded as projects that succeed.

Companies currently operating at a loss may also benefit, because federal R&D credits generated but not used can be carried back one year and forward up to 20 years creating an opportunity when the company becomes profitable. Additionally, for tax years beginning in 2016, startup companies with less than $5 million in revenue can use the R&D credits against their payroll tax if they have no income tax liability. Taxpayers in alternative minimum tax (AMT) situations can use R&D credits against their individual AMT, if applicable. Furthermore, if the company is acquired, the credits can be considered a valuable future asset in negotiating a selling price for the business.

Properly calculating and substantiating the R&D tax credit is critical for maximizing financial benefits and sustainability. Detailed employee and project time tracking data will help facilitate nexus considerations. Documentation in the software industry is usually abundant, as projects are generally closely tracked and monitored from start to finish. Records are normally kept contemporaneously within the system. These are key ingredients for a successful R&D tax credit claim.

Qualified companies doing a cost-benefit analysis on claiming R&D tax credits should consider the fact that most states also offer their own R&D tax credits which require similar documentation to the federal credit, thereby potentially increasing the benefits side of the equation. This article offers specific examples of qualifying and non-qualifying activities in the cybersecurity industry through the case studies below.

Case Studies: Cybersecurity Industry Client Examples

The following are case studies that further illustrate the types of projects and activities that will potentially qualify for the R&D tax credit in the cybersecurity industry. The eligibility of specific activities and expenditures will depend on a closer examination of the facts and circumstances in relation to applicable guidance.

CASE 1: Company A sought to create a wholly new set of cybersecurity software tools and features to fully replace an existing stack of malware protection. The company's IT and cybersecurity team was unsure if it had the capability to design a component of architecture. Initial schematics were drafted and reviewed by the implementation team. They evaluated several alternative solutions to address web-based attacks, phishing/social engineering attacks, SQL injections, and ransomware. After a systems analysis they created a proof of concept and began development. The IT team created enhanced authorization functions through improved software design, code optimization, and logic engine design. Then the cybersecurity team evaluated the malware firewalls to ensure the code will function properly. There was extensive non-routine trial and error testing, researching, and refining the software to determine the appropriate model of the final solution. Company A may qualify for the credit due to the technical security uncertainties the IT and cybersecurity team faced while creating a new design component.

CASE 2: Company B is a cybersecurity firm that develops software for external users. The company analyzes existing software to find design flaws to create a more secure and functional product. To do this, a programmer performs trial and error testing of the software to identify the corrupt code. Subsequently, the developer will write improved code, create secure software tools, and undergo a rigorous quality assurance and testing process to create enhanced software solutions in the hopes of selling to the public. The new architecture design, software development and modification, and beta testing are just a few examples that may qualify for the R&D tax credit given the technological uncertainty of solving the code and the trial and error process of experimentation.

How Does the R&D Tax Credit Work?

The R&D tax credit is available to taxpayers who incur incremental expenses for qualified research activities (QRAs) conducted within the U.S. The credit is comprised primarily of the following qualified research expenses (QREs):

1. Internal wages paid to employees for qualified services. Wages are defined to include amounts considered to be wages for federal income tax withholding purposes. Sections 41 (b)(2)(D)(i) and 3401(a).

2. Supplies used and consumed in the R&D process. Supplies are defined as any tangible property other

than land or improvements to land, and property subject to depreciation. Section 41 (b)(2)(C).

3. Contract research expenses (when someone other than an employee of the taxpayer performs QRAs on behalf of the taxpayer, regardless of the success of the research). Section 41(b)(3).

4. Basic research payments made to qualified educational institutions and various scientific research organizations. Section 41(b)(3)(C).

For an activity to qualify for the research credit, the taxpayer must show that it meets the following four tests:

1. The activity must rely on a hard science, such as engineering, computer science, biological science, or physical science.

2. The activities must relate to the development of new or improved functionality, performance, reliability, or quality features of a structure or component of a structure, including product or process designs that a firm develops.

3. Technological uncertainty must exist at the outset of the activities. Uncertainty exists if the information available at the outset of the project does not establish the capability or methodology for developing or improving the business component, or the appropriate design of the business component.

4. A process of experimentation (e.g., an iterative testing process) must be conducted to eliminate the technological uncertainty. This includes assessing a design through modeling, computational analysis or trial and error testing.'

Once it is established that the activities qualify, a thorough analysis must be performed to determine that the taxpayer has assumed the financial risk associated with (Treas. Reg. 1.41-2(e)(2).), and will have substantial rights to (Treas. Reg. 1.41-2(e)(3); *see also Lockheed Martin Corp. v. United States*) the products or processes that are developed through the work completed. The next step is to develop a methodology for identifying, quantifying, and documenting project costs that may be eligible for the R&D credit. Costs that qualify for the credit include wages of employees involved in developing new or improved products or processes, supplies used or consumed during the research process, and 65 percent of fees paid to outside contractors who provide qualifying R&D services on behalf of the taxpayer.

Determining the true cost of R&D is often difficult because few companies have a project accounting system that captures many of the costs for support provided by the various personnel who collaborate on R&D. The typical project tracking system would not include contractor fees, direct support costs, and salaries of high-level personnel who participate in the research effort.

Appropriate documentation may require changes to the company's recordkeeping processes because the burden of proof regarding all R&D expenses claimed is on the taxpayer. The company must maintain documentation to illustrate nexus between QREs and QRAs. According to the IRS Audit Techniques Guide for the R&D credit, the documentation must be contemporaneous, meaning that it was created in the ordinary course of conducting the QRAs. Furthermore, a careful analysis should take place to evaluate whether expenses associated with eligible activities performed in the company outside of the R&D department may have been missed and can be included in the R&D tax credit calculation. This is accomplished by interviewing personnel directly involved in R&D or those who support or supervise R&D efforts.

Internal Use Software (IUS):

Cybersecurity companies as well as companies with potential exposure to security threats continue to invest resources in the design and development of internal use software to combat these threats. In claiming the R&D tax credit, taxpayers may include expenses incurred for developing a completely new software for use by third parties or extensive improvements to existing internal use software. As such, companies revamping and updating their own malware protection system may qualify for the credit.

The Treasury and IRS regulations released on Oct. 3, 2016 that clarified the definition of IUS. These final regulations contain several important changes related to the definition of IUS, the definition of ''high threshold of innovation,'' and offer additional guidance for claiming the R&D tax credit for IUS expenditures. These are a welcoming change for cybersecurity experts who spend significant resources developing internal use software.

While these regulations are favorable for taxpayers that significantly update or improve internal software components, companies and accountants need to be aware of potential exclusions. The final regulations state that whether software is or is not developed primarily for internal use depends on the taxpayer's facts and circumstances at the beginning of the software development. If a taxpayer originally develops software primarily intended for internal use but later makes improvements to the software with the intent to hold the improved software for commercial sale, lease, or license, or to allow third parties to initiate functions or review data on the taxpayer's system, the improvements will be considered separate from the existing software and will not be considered developed primarily for internal use.

In addition to the four tests, if development is conducted related to IUS, there are an additional three tests that must be satisfied. Software developed by the taxpayer that is considered to be IUS must meet the additional three-part test in addition to the four-part test to qualify for the R&D tax credit. The additional three requirements are:

1. The software must be innovative. (It results in a reduction in cost or an improvement in speed that is substantial and economically significant.)

2. Developing the software involves significant economic risk. (The taxpayer commits substantial resources to software development and, due to technical risk, there is substantial uncertainty that it will recover the resources in a reasonable period.)

3. The software is not commercially available. (The taxpayer cannot purchase, lease, or license and use the software for the intended purpose without modifications that satisfy the first two requirements.)

Historically, the regulations for IUS were ambiguous at best. The final regulations clarified the definition of IUS, which is now defined as software developed by the taxpayer for general and administrative functions that facilitate or support the conduct of the taxpayer's trade or business. These general and administrative functions are limited to human resource management, financial

management, and support services functions. This is to be distinguished from commercial software, which is developed to be commercially sold, leased, licensed, or otherwise marketed to third parties, and software that is developed to enable a taxpayer to interact with third parties or to allow third parties to initiate functions or review data on the taxpayer's system.

The final regulations clarify that internally developed software is considered innovative if the development would result in a substantial and economically significant reduction in cost, improvement in speed, or other measurable improvement. The regulations also reiterate that significant economic risk exists only if the taxpayer commits substantial resources to the development and the likelihood that such resources will be recovered within a reasonable period is substantially uncertain. In defining substantial uncertainty, the final regulations note that the uncertainty must relate to the capability or methodology, but not the appropriate design of the business component to create a higher threshold for eligibility than Congress originally intended for IUS.

Cybersecurity Industry Examples of Qualifying and Non-qualifying R&D Activities

Qualifying R&D activities as they apply to the cybersecurity industry generally fall within four general buckets: (1) new product development; (2) incremental product improvement; (3) new process development; and (4) incremental process improvement.

Examples of qualifying activities include:

1. Design or development of any new cybersecurity software or technology products for commercial sale, lease, or license.
2. Cybersecurity software developed as part of a hardware/software product (embedded software).
3. Modification or improvement of existing cybersecurity software or technology platform that significantly enhances performance, functionality, reliability, or quality.
4. New architecture design.
5. Programming cybersecurity software source code.
6. Research of specifications and requirements, cybersecurity software elements, including definition of scope and feasibility analysis for development or functional enhancements.
7. Beta testing—logic, data integrity, performance, regression, integration, or compatibility testing.
8. Optimization of cybersecurity software source code for better performance, new functionality, or integration with new platforms or operating systems.
9. Research for development of applications for cybersecurity technology patents.

Examples of activities that will not qualify for purposes of the R&D credit include:

1. Routine testing or inspection activities for qualify control.
2. Developments related entirely to aesthetic properties of a cybersecurity software package.
3. Routine bug fixes.
4. Market research for advertising or promotions.
5. Routine data collections.
6. Research conducted outside of the U.S., Puerto Rico, or any possession of the U.S.
7. Research that is funded by a third party other than the taxpayer.
8. Any other activities that do not meet all of the four tests as previously outlined.

Conclusion

Product and process development and innovation are the main drivers of the R&D tax credit. Businesses have more to gain than ever before for pushing the envelope to create improved technology solutions aimed at keeping us safe online. The research credit can provide meaningful benefits to qualified companies by driving down effective tax rates, generating cash flow, and reducing the cost of research and development. In addition, benefits may be claimed at both the federal and state level.

Yair Holtzman is a Tax Partner at Anchin, Block, and Anchin, R&D Tax Credits and Incentives Practice Leader and is also the leader of the Chemicals & Energy and Life Sciences Practice Industry Groups. Melissa Cohen *is a Senior Associate in the R&D Tax Credits and Incentives practice group at Anchin.* Alex Okin *is an Associate in the R&D Tax Credits and Incentives practice group at Anchin.*