Articles in the Journal of Equipment Lease Financing are intended to offer responsible, timely, in-depth analysis of market segments, finance sourcing, marketing and sales opportunities, liability management, tax laws regulatory issues, and current research in the field. Controversy is not shunned. If you have something important to say and would like to be published in the industry's most valuable educational journal, call 202.238.3400.

Editorial Board

Economic Effect and Possible Mitigating Actions of a Tax Rate Increase on Existing Tax Lease Transactions
By Raymond James

Leading up to the 2020 election, the Democratic party promised an increase in the federal corporate tax rate from 21% to 28%. That could happen before the 2022 midterm elections. What would be the effect of that increase on tax-advantaged equipment leases booked under the 21% rate? Here are some scenarios that can be used to model potential alternatives.

Working from Home: A Hacker's Perspective
By Joseph Granneman

The best way for companies to defend their remote workers and their organizations is to start thinking like a cybercriminal. Employees are isolated, often with reduced communication about critical business processes. As this article details, any discussion about preventing cyberfraud should address areas of potential weakness as well as remediation options.

JOURNAL

OF EQUIPMENT LEASE FINANCING

Economic Effect and Possible Mitigating Actions of a Tax Rate Increase on Existing Tax Lease Transactions

Leading up to the 2020 election, the Democratic party promised an increase in the federal corporate tax rate from 21% to 28%. That could happen before the 2022 midterm elections. What would be the effect of that increase on tax-advantaged equipment leases booked under the 21% rate? Here are some scenarios that can be used to model potential alternatives.

By Raymond James

This article showcases a study examining the effects that a federal corporate tax rate change could have on tax-advantaged equipment leases originated when the federal corporate tax rate was 21%, should the tax rate be increased to, for example, 28%.

In addition, the article discusses some of the potential effects of a tax rate increase and the possible actions that lessors may take to mitigate or minimize the risk associated with a tax rate increase.

This article illustrates how the after-tax return on equity would drop from a positive 13.32% to a *negative* 7.80% should the federal corporate tax rate be increased from 21% to 28%.

BACKGROUND

While the drop in the federal corporate tax rate from 35% to 21% initiated in 2017 arguably spurred economic growth, it also arguably caused an increase in the national debt as well as observations that it was an unfair giveaway to corporations.

As a result of these beliefs, leading up to the 2020 election, the Democratic party promised an increase in the federal corporate tax rate to 28% — which happens to be the midpoint between 35% and 21% — as one means of paying for the party's extensive spending proposals.[1,2]

During the Biden administration, there is no guarantee of when a rate change might occur nor the magnitude. A change in power in Congress away from the party winning the presidential election is often experienced in the midterm elections. However, if the current administration is able to obtain the votes needed for a change, a tax rate increase may occur prior to the midterm elections, now less than two years away.

All of the analyses herein use a 28% federal corporate tax rate as the comparison to the current 21% rate, since we do not have a better number to use at this time.

As of this writing, it is not known whether an increase in the federal corporate tax rate can be passed nor what the new rate would be.[1,2] Furthermore, other measures could be implemented such as a flat tax or a revised alternative minimum tax (AMT). Nonetheless, a worthwhile exercise is to examine the effect a rate increase would have on existing tax-oriented leases — as well as those written between now and when a rate increase occurs.

Secondarily, exploring what potential actions a lessor could take to mitigate the potential impact of such an increase on yields and profits is also worthwhile.

DISCUSSION AND ANALYSIS

All of the analyses herein use a 28% federal corporate tax rate as the comparison to the current 21% rate, since we do not have a better number to use at this time. The parameters for all seven examples are included under Example 1, below.

Rather than save the "punchline" as to how we arrived at it for after the discussion, we are presenting the results in Table 1.

A tax rate increase that would negatively affect transactions that were priced and booked under a 21% tax rate where 100% bonus depreciation was taken creates a substantial increase in income tax paid versus what was calculated at the time of booking.

This situation is caused by the tax benefit of 100% bonus depreciation being taken under a 21% tax rate and leaves the remaining rental payments without depreciation to offset them. Thus, the rental income and future sale of the asset would be taxed at a higher tax rate.

The examples in this study attempt to quantify the effect of a higher tax rate and then measure the impact of possible mitigating alternatives.

Table 1.

Highlights from the Article

Metric	Status quo 21% rate claiming 100% bonus; no tax rate increase	Do nothing Effect of tax rate increase to 28% in 2022 on status quo (claiming 100% bonus)	No bonus with rate increase Effect of NOT claiming bonus and ASSUMING a tax rate increase	No bonus no rate increase Effect of NOT claiming bonus and assuming NO tax rate increase
IRR	4.10%	4.10%	4.10%	4.10%
Taxes paid	$22,400	$92,809	$36,809	$22,400
AT cash/profit	$84,270	$13,861	$69,861	$84,270
AT MISF	4.00%	0.69%	2.94%	3.47%
AT ROE	13.32%	-7.80%	7.17%	9.75%

Source: Raymond James, Ivory Consulting, using SuperTRUMP software (all tables).

A significant benefit can be realized from one mitigating effect: not taking 100% bonus depreciation on transactions priced using a 21% tax rate booked in 2021.

Equipment Leasing and Finance Association members who participated in the 2020 and 2021 Survey of Equipment Finance Activity covering the years 2018, 2019 and 2020 averaged booking approximately $32 billion each year, or 30% of their new business volume, as tax-advantaged leases under a 21% tax rate.

The data from these three years is important because they were the first three years of the historically low 21% federal corporate tax rate and the 100% bonus depreciation option.

The 21% tax rate provided less incentive to book tax-advantaged leases. However, 100% bonus depreciation happened to essentially offset the advantages of tax leasing for lessors.

In this study, the metrics used to measure the impacts are actual taxes paid without an increase versus with the proposed tax increase. Changes to the economic Multiple Investment Sinking Fund (MISF) yield and return on equity (ROE) yield are also explored.

Both yields are expressed as after-tax (AT) yields, while the internal rate of return (IRR) and cost of funds (COF) are expressed as pre-tax (PT) yields. The need and quantification of a tax-indemnification agreement is considered from both a full-term and an early termination perspective.

The analysis performed in this study looks at a lease booked in 2021, which is expected to end four years later with the asset ultimately sold. It is a 48-month, $1,000,000, tax-advantaged lease booked July 1, 2021, priced using a 21% tax rate with 100% bonus depreciation and assuming a 30% residual value, resulting in a 4.10% IRR.

Assuming the proposed increase in the 2022 federal corporate tax rate from 21% to 28% is taken into consideration, the taxes paid over the transaction's life increase from $22,400 to $92,809, or 4.14 times greater. The economic effect is to reduce the AT MISF from 4.00% to 0.91% and the ROE from 13.32% to *negative* 7.80%.

A significant benefit can be realized from one mitigating effect: not taking 100% bonus depreciation on transactions priced using a 21% tax rate booked in 2021. If 5-year MACRS depreciation is the only depreciation used, the increase in taxes paid is only 1.64 times greater, the AT MISF drops more moderately from 4.00% to 2.94%, and the ROE falls from 13.32% to a more acceptable 7.17%.

The risk in using this mitigating factor is that the tax rate remains at 21% indefinitely. Then the AT MISF and the ROE yields will be lower because of the deferral of depreciation, which would otherwise have been taken as 100% bonus. The pre-tax IRR remains the same.

Given the significant beneficial impact of not taking 100% bonus depreciation in 2021, lessors might give serious consideration to advanced tax planning now. The summary below presents the basis for the first example.

EXAMPLE 1. BASE CASE: FEDERAL CORPORATE TAX RATE REMAINS AT 21%

Assumptions

- *No federal corporate tax increase*
- Booked and funded: July 1, 2021
- Equipment cost: $1,000,000
- Depreciation: MACRS 5-year
- Bonus depreciation: 100% first year
- Term: 48 months (monthly in advance)
- Payment: $16,805.64
- Residual: 30%
- COF pretax: 3.00%
- Tax rate: 21%

Results

- IRR (pre-tax nominal): 4.10%
- MISF (after-tax nominal): 4.00%
- ROE (after-tax economic @ 85% leverage): 13.32%
- Tax paid: $22,400
- After-tax cash/profit: $84,270

Two simple reports shown in Table 2 and Table 3 illustrate what drives these results:

In the first year, 100% bonus depreciation more than offsets the small amount of rental income, leaving a tax benefit of $188,825

to offset other enterprise income in 2021. The following years have the balance of the rental income plus the tax gain on the residual value, which is fully taxable at 21% without any offsetting depreciation.

The bottom line is $106,672 of taxable income and $22,400 in taxes. The delayed payment of taxes is what ultimately led to an 4.00% AT MISF and a 13.32% ROE.

The cash-flow report (Table 2) was fed by the tax report above. It is presented in this example only to illustrate the final after-tax cash flows supporting the MISF calculation. *Further analyses will not present the cash-flow report, to avoid repetition.*

EXAMPLE 2. FEDERAL CORPORATE TAX RATE INCREASES TO 28%

The following example illustrates the results of a federal corporate tax rate increase to 28% effective January 1, 2022, for business booked in 2021 under a 21% rate, while maintaining all other assumptions.

Assumptions

- *Federal corporate tax rate increases to 28% effective January 1, 2022.*
- All other assumptions stay the same.

Results

- IRR (pre-tax nominal): 4.10%
- MISF (after-tax nominal): 0.69%

- ROE (after-tax economic @ 85% leverage):-7.80%
- Tax paid: $92,809
- After-tax cash/profit: $13,861

In order to understand what happened, it is best to look at the tax report generated under this new assumption (Table 4).

Table 2.

Tax Report: Federal Corporate Tax Rate Stays at 21% and 100% Bonus Depreciation

Period ending	Rent	+	Residual	-	Depreciation	=	Taxable income	Rate 21.0%*	=	Tax due/paid
12/30/2021	100,834		-		1,000,000		(899,166)	21		(188,825)
12/30/2022	201,668		-		-		201,668	21		42,350
12/30/2023	201,668		-		-		201,668	21		42,350
12/30/2024	201,668		-		-		201,668	21		42,350
12/30/2025	100,834		300,000		-		400,834	21		84,175
Total	**806,672**		**300,000**		**1,000,000**		**106,672**			**22,400**

Table 3.

Cash-Flow Report: Federal Corporate Tax Rate Stays at 21% and 100% Bonus Depreciation

Period ending	Rent	+	Residual	-	Asset cost	=	Pretax cash	-	Tax paid	=	After-tax cash
12/30/2021	100,834		-		1,000,000		(899,166)		(188,825)		(710,341)
12/30/2022	201,668		-		-		201,668		42,350		159,317
12/30/2023	201,668		-		-		201,668		42,350		159,317
12/30/2024	201,668		-		-		201,668		42,350		159,317
12/30/2025	100,834		300,000		-		400,834		84,175		316,659
Total	**806,672**		**300,000**		**1,000,000**		**106,672**		**22,400**		**84,270**

Table 4.

Tax Report: Federal Corporate Tax Rate Increases to 28% January 1, 2022, and 100% Bonus Depreciation

Period Ending	Rent	+	Residual	-	Depreciation	=	Taxable income	Rate*	=	Tax due/paid
12/30/2021	100,834		-		1,000,000		(899,166)	21		(188,825)
12/30/2022	201,668		-		-		201,668	28		56,467
12/30/2023	201,668		-		-		201,668	28		56,467
12/30/2024	201,668		-		-		201,668	28		56,467
12/30/2025	100,834		300,000		-		400,834	28		112,233
Total	**806,672**		**300,000**		**1,000,000**		**106,672**			**92,809**

The most powerful way to mitigate the effect of a federal corporate tax rate increase in 2022 on business booked in 2021 is to not *take bonus depreciation in 2021 and to use only MACRS depreciation.*

It is immediately apparent why taxes due rose sharply from the 21% to 28% corporate tax rate change. Much of what is driving this change comes from taking the 100% bonus in 2021, when the transaction was booked, leaving no depreciation to offset future rent and a residual value income gain. Therefore, these income items must be taxed at the new rate of 28%, which caused the taxes paid to increase significantly — from $22,400 to $92,809.

POSSIBLE ACTIONS TO MITIGATE OR MINIMIZE THE EFFECT

Mitigating the Effect of the Potential Federal Corporate Tax Rate Increase in 2022 for Lease Transactions Booked in 2021

The most powerful way to mitigate the effect of a federal corporate tax rate increase in 2022 on business booked in 2021 is to *not* take bonus depreciation in 2021 and to use only MACRS depreciation.

This election allows depreciation to be expensed over more years and offset against income in those years when the federal corporate tax rate could be 28%. A series of tables

have been designed to show the effect on the above example with various changes, as noted below.

EXAMPLE 3. NOT TAKING 100% BONUS DEPRECIATION AND THE TAX RATE INCREASES AS OF JANUARY 1, 2022

Table 5 illustrates the benefit of using 5-year MACRS instead of 100% bonus depreciation. The AT MISF increases from 0.69% to 2.94%, while the related profit increases from $13,861 to $69,861. Similarly, the ROE increases from -7.80% to 7.17%.

EXAMPLE 4. NOT TAKING 100% BONUS DEPRECIATION AND THE TAX RATE INCREASES AS OF JANUARY 1, 2023

If the proposed tax rate increase is delayed a year and is increased effective January 1, 2023, applicable to business booked in 2021 under a 21% rate, then the results are as shown in Table 6.

By not taking the 100% bonus depreciation in 2021 and using 5-year MACRS, the results are again

---

Table 5.

Business Booked in 2021

	IRR	AT MISF	AT ROE	PT profit	Tax paid	AT profit
Rate changes 2022 to 28% - 100% bonus taken	4.10%	0.69%	-7.80%	$106,672	$92,809	$13,861
- 5 year MACRS no bonus	4.10%	2.94%	7.17%	$106,672	$36,809	$69,861

better. The AT MISF increases from 1.39% to 2.58%, while the related profit increases from $27,978 to $61,578. Similarly, the ROE increases from -3.50% to 4.42%.

Note: These results are the same as new business booked July 1, 2020, with the rate increasing in 2022 to 28%. In both instances, there are 18 months of income realized at 21% followed by 30 months of income realized at 28%.

EXAMPLE 5. NOT TAKING 100% BONUS DEPRECIATION AND THE TAX RATE DOES NOT INCREASE

The last scenario to be considered is a review of the results if the federal corporate tax rate does not change.

Table 7 shows the cost of *not* taking the 100% bonus depreciation and instead using 5-year MACRS. The AT MISF decreases from 4.00% to 3.47%, and the ROE decreases from 13.32% to 9.75%.

Similarly, the related *after-tax profit stays the same.* The reason it does not change is that bonus depreciation only improves the yields related to the timing of tax benefits, not actual taxes paid, in a static tax rate environment.

Mitigating the Federal Corporate Tax Rate Increase in 2022 by Having the Customer Pay
The adverse impact on the earnings of a tax lease, due to a federal corporate tax rate increase from 21% in 2021 to something higher in 2022 or beyond, could be borne by the lessee. Asking a lessee may

Table 6.

Business Booked in 2021

	IRR	AT MISF	AT ROE	PT profit	Tax paid	AT profit
Rate changes 2023 to 28% - 100% bonus taken	4.10%	1.39%	-3.50%	$106,672	$78,693	$27,978
- 5 Year MACRS no bonus	4.10%	2.58%	4.42%	$106,672	$45,093	$61,578

Table 7.

Business Booked in 2021

	IRR	AT MISF	AT ROE	PT profit	Tax paid	AT profit
Rate stays at 21% - 100% bonus	4.10%	4.00%	13.32%	$106,672	$22,401	$84,270
- 5 year MACRS no bonus	4.10%	3.47%	9.75%	$106,672	$22,401	$84,270

One caution to lessors: write tax-indemnity language in such a way that it applies the additional costs of the tax rate change to any early buyout or early termination.

be difficult, but as the likelihood of a rate increase grows, lessors may become more emboldened to consider this as part of the lessee-lessor bargain.

This transfer of obligation has been typically done with indemnification language in the lease agreement. There are perhaps several ways the transfer of obligation could be structured. Two are:

• Periodic lease payments are increased during the periods in which the tax rate increases.

• A one-time payment is required at the end of the lease, no matter the form of termination.

The second item to consider would be the metric to use for determining the amount of the transfer of obligation:

• Protecting the AT MISF yield or the ROE yield used when the lease was originally priced and executed

• Protecting the AT Cash/Profit to the extent it is impacted by the tax rate change

One caution to lessors: write tax-indemnity language in such a way that it applies *the additional costs of the tax rate change to any early buyout or early termination.* Without including tax indemnity on early terminations, smart lessees will end their leases early and enjoy much better terms with a new lease written in a 28% federal corporate tax rate environment

compared with paying a tax indemnity reimbursement at the end of an existing lease.

Below is an example of how a tax rate change indemnification could be executed based on examples 1 and 2.

EXAMPLE 6. TAX RATE CHANGE INDEMNIFICATION

Table 8 shows how much more the lessee must pay in order to compensate the lessor with the federal corporate tax rate increase to 28% effective January 1, 2022. The additional amount paid by the lessee is more than might be expected by the IRR, almost doubling from 4.00% to approximately 7.50%.

Without after-tax pricing, the effect of 2021 or earlier bonus depreciation taken in a 21% environment is difficult to measure. The IRR provided here is one of the few metrics that the lessee will likely be able to use to quantify the cost as it is easily calculated because it is a pre-tax number.

For example, the lessee may likely know the price of the equipment being leased, the payments in the lease, an EBO (Equitable Business Opportunities) number, and price cap on the residual or fixed-price option. A simple financial calculator or Excel spreadsheet could then produce the IRR yield.

The profitability of transactions that might be booked in 2022 under a federal corporate tax rate of 28% is not nearly as adversely affected as those booked in 2021 under a federal corporate tax rate of 21%.

Lessor Considerations if the Federal Corporate Tax Rate Increases in 2022 for Business Booked in 2022

The profitability of transactions that might be booked in 2022 under a federal corporate tax rate of 28% is not nearly as adversely affected as those booked in 2021 under a federal corporate tax rate of 21%.

An additional consideration for analysis is bonus depreciation, which is scheduled to drop from 100% in 2022 to 80% in 2023. Below are the economic results from these changes.

EXAMPLE 7. TAX RATE CHANGE PLUS BONUS DEPRECIATION RATE CHANGE

Looking at Table 9, when the tax rate is 28% and 100% bonus depreciation is taken, both the AT

Table 8.

Tax Rate Indemnification Alternatives Explored

	IRR	AT MISF	AT ROE	AT profit
Rate stays at 21% - 100% bonus	4.10%	4.00%	13.32%	$84,270
Rate changes 2022 to 28% - 100% bonus	4.10%	0.69%	-7.80%	$13,861
Payment adjustment alternative:				
2021 payments (1-6)	$16,805.64	$16,805.64	$16,805.64	$16,805.64
2022 payments and beyond (7-48)	$16,805.64	$19,071.62	$18,971.42	$16,805.64
One-time payment at the end		$-	$-	$97,790
Pre-tax profit/cash (rent+residual-investment)		$201,842	$197,633	$204,461
Taxes paid		$(119,457)	$(118,279)	$(120,191)
AT cash/profit		$82,385	$79,354	$84,270
Resultant metrics	4.10%	4.00%	13.32%	$84,270
NOTE: Lessee's perceived IRR w/ tax indemnity		7.62%	7.47%	7.20%

Table 9.

Business Booked in 2022/2023

	IRR	AT MISF	AT ROE	PT profit	Tax paid	AT profit
Rate changes 2022 to 28% - 100% bonus taken	4.10%	3.95%	14.23%	$106,671	$29,868	$76,803
Rate changes 2022 to 28% - 80% bonus taken	4.10%	3.77%	13.11%	$106,671	$29,868	$76,803

Ultimately, lessors that offer tax-advantaged leases will need to ensure they look at all the costs of a federal corporate tax rate change via modeling various potential alternatives.

MISF and ROE change slightly from what they are under the current 21% federal corporate tax rate. AT MISF decreases from 4.00% to 3.95% and ROE increases from 13.32% to 14.23%.

The after-tax profitability in 2022 is lower than what it is under the current 21% federal corporate tax rate. After-tax profits of $84,270 become $76,803. If bonus depreciation is limited to 80% for business booked in 2023, then the AT MISF decreases from 3.95% to 3.77% and the ROE falls from 14.23% to 13.11%, as shown above.

CONCLUSIONS

The primary purpose of this study was to investigate the impact on lessor profits from tax-advantaged equipment leases booked under the recent 21% federal corporate tax rate should the rate be increased in 2022 to 28% — consistent with the 2020 Democratic party platform. The impact of the tax rate change(s) will vary depending on a number of factors that include:

- timing and magnitude of the tax rate increase and/or bonus depreciation change via lessor election
- structure of the leases: term, payment structure, etc.
- state taxes

Ultimately, lessors that offer tax-advantaged leases will need to ensure they look at all the costs of a federal corporate tax rate change

via modeling various potential alternatives. They will need to review those potential alternatives with skilled internal tax staff or with a consultant who can accurately analyze all the specifics related to a given corporate situation.

In addition, where possible, lessors may want to employ tax-indemnification language in their lease agreements so that they are protected from adverse tax costs arising out of either a full-term or early termination.

No attempt has been made to assign any probability to the various examples and scenarios in this article. There are so many other possibilities that could develop beyond the examples presented here.

After-tax pricing software designed for use by the equipment finance industry allows a user to produce tax-related scenarios with a few minutes of inputting assumptions. Thus, it is suggested that lessors work with those who follow the probabilities of various potential changes in the future federal corporate tax laws — including no change at all.

Scenarios can be easily constructed to model and answer many what-if questions, to come to a consensus on how to handle various tax elections, pricing changes, and quantification of a tax-indemnification clause for each of the financial products offered by a lessor in 2021 and beyond.

Endnotes

1. Alan Rappeport, "The Biden administration seeks to raise $2.5 trillion through corporate tax increases," *New York Times,* April 7, 2021.

2. Theo Francis and Richard Rubin, "A 28% Tax Rate Will Cost Companies, but Not Equally," *Wall Street Journal,* April 5, 2021.

Raymond A. James

Ray.james@ivorycc.com

Raymond James, based in Chicago and Fort Myers, Florida, has served since 2006 as senior consultant for Ivory Consulting Corp. in Walnut Creek, California. He started his finance career in commercial loans for the National Bank of Detroit then held managerial positions at Chrysler Corp., Computer Sciences Corp., the Upjohn Co., and Senstar Capital Corp. Senstar was sold to John Deere Financial in 1999. For the next six years, Mr. James worked at John Deere Financial as a director of various areas, including strategic planning, mergers and acquisitions, business development, corporate pricing and syndication. He retired from John Deere Financial in 2005. Mr. James is the recipient of the ELFA's 2016 Michael J. Fleming Distinguished Service Award. He has served on the Research Committee since 1991 and is the current chair. As a pioneering member of the Research Committee, he has helped the Survey of Equipment Finance Activity (SEFA) report grow into ELFA's signature benchmarking and research tool. Mr. James graduated from Eastern Michigan University in Ypsilanti with a BS in mathematics and economics and from Wayne State University in Detroit with a MA in econometrics.

Working from Home: A Hacker's Perspective

The best way for companies to defend their remote workers and their organizations is to start thinking like a cybercriminal. Employees are isolated, often with reduced communication about critical business processes. As this article details, any discussion about preventing cyberfraud should address areas of potential weakness as well as remediation options.

By Joseph Granneman

The COVID 19 pandemic has impacted our professional and personal lives in many ways. Business models shifted to online services in almost every business niche, or vertical. Retail shopping, grocery delivery, and even religious services moved to online platforms. Businesses quickly shifted their office operations online, with many employees quickly sent home to work remotely using their existing consumer-grade hardware.

There will be some return to the physical workplace for many of these services, once people start to transition to a post-COVID world. However, many employers and employees are not in a rush to return to the office anytime soon. Working from home may be one of the changes the pandemic leaves behind along as part of a new definition of *normal.*

Cybercriminals, having taken notice of the new remote working model, have adapted their

techniques to be more effective in this new paradigm. Working remotely increases opportunities for cybercriminals, as many of the defenses available in the office are no longer available otherwise.

Remote employees become more dependent on technology and interconnectivity, which are then targeted by cybercriminals. With employees isolated, communication between staff members about critical business processes is reduced — potentially exposing the opportunity for fraud.

The best way for companies to defend their remote workers and their organizations is to start thinking like a cybercriminal. It is critical to identify not only the potential technical vulnerabilities but also threats from the physical environment and social engineering.

This article will examine some areas of potential weakness and remediation options to kickstart these discussions. This

Critical business processes that involve the transfer of funds also need to be shored up with manual approval and verification processes. Never rely solely on email communications.

article is not intended to be an all-inclusive list. Security teams should conduct their own threat-modeling exercises to identify specific vulnerabilities of their own organization.

SOCIAL ENGINEERING

Phishing is still the most popular form of social engineering and the most common cyberattack. Criminals continue to find success by sending fake email links to malicious websites or fraudulent invoices. Although phishing is a big enough problem for employees working at the office, it can be even more so for those working remotely.

For example, there is a level of distraction when working remotely that reduces the level of diligence that employees must exercise to identify fraudulent messages. Employees are more comfortable working from home and may not be as cautious in this environment as they would have been in the office.

Increased technology usage in the home office creates more targets for phishing remote employees. An organization that allows the employee to "bring your own device" (BYOD) can be especially hazardous. Family members may use the shared family computer for other tasks and get phished through other means such as social networks, instant messengers, and personal email accounts.

The attacker may still gain access to the network through a family member, even if they use a separate computer, and launch an attack against the employee. They could recover the password to the Wi-Fi network from a family member's computer, for example. Many attackers will target family members of company VIPs for this very reason.

Training and Device Management

Training and device management are key to defending remote employees against these types of social-engineering attacks. As the rush to send people home in response to COVID overrode information security concerns, many companies implemented remote-work programs without sufficient training. Employees must be continually reminded and tested on recognizing phishing, including threats that come from non-company-related sources such as social media or personal email.

Critical business processes that involve the transfer of funds also need to be shored up with manual approval and verification processes. Never rely solely on email communications.

BYOD should actually stand for "bring your own data breach": the risk of using personally owned computer systems for business is almost untenable. Organizations should own and manage the personal computer equipment that is used for their business processes. These systems should not be shared with family members or used for any personal business.

Home firewalls also allow for insecure practices for other consumer-grade technology. The employee's child may play games on an Xbox that requires inbound network traffic.

Personal smartphones and tablets that can be managed through mobile device management (MDM) tools are the only exceptions. MDM on Windows computers is far less effective while being more intrusive on a personally owned computer. Companies will find that providing a company-owned Windows desktop instead will improve both employee satisfaction and cost savings in the long run.

CONSUMER GRADE TECHNOLOGY

An organization that provides a company-owned computer for its employees working from home has other risks that need to be considered. An often-overlooked risk — one of the most critical — is the consumer-grade technology that comprises the employee home network. For example, enterprise firewalls used by organizations to protect their networks have cutting-edge features and are frequently updated.

By contrast, firewalls used in homes are usually disposable units (under $100) that came from a retail store and run old versions of Linux, with basic inbound traffic blocking and no updates. Home firewalls typically allow all outbound network traffic, whereas enterprise firewalls require specific rules.

Home firewalls also allow for insecure practices for other consumer-grade technology. The employee's child may play games on an Xbox that requires inbound network traffic. Home firewalls support a protocol called Universal Plug and Play (UPnP), which allows the game to initiate opening the inbound firewall ports. This can expose the home network to inbound network traffic that in turn could expose the company-owned computer to potential security risks.

Attackers may also trigger UPnP to add additional inbound rules to the firewall once a computer has been compromised initially. This allows an attacker direct access into a home computer by effectively bypassing the firewall for all remote connections.

Web Content Filtering and Logging

Home firewalls also lack the capability of providing web content filtering and logging. Most organizations utilize some type of web content filter on their network that prevents access not only to objectionable content but also to malicious websites. The company-owned computer on this type of home network may be exposed to web-based malware that would have been prevented in the office. The lack of web-content filtering and logging also means that the organization will not have these logs for use in incident response.

A Shorter Life Span

The life span of home network equipment including firewalls, switches, and wireless routers is far shorter than their business-class counterparts. Most home users

Consumer network equipment has another potential security vulnerability in the way it is managed. Many technology companies are linking these devices through cloud-based services to allow for configuration from a smartphone.

purchase their home equipment and never run updates; nor are they even aware of when their equipment is unsupported.

Criminals are scanning the internet repeatedly for flaws in many of these outdated consumer firewalls that allow for full remote administrative control. They can use these compromised devices to attack the home workstations and potentially steal data through network traffic analysis. These old firewalls are commonly used as nodes in distributed denial of service (DDoS) attacks by criminals against other targets.

Consumer network equipment has another potential security vulnerability in the way it is managed. Many technology companies are linking these devices through cloud-based services to allow for configuration from a smartphone.

Multi-Factor Authentication
Remote workers may not set the best passwords for these sites and seldom enable multi-factor authentication (MFA). Attackers can test simple passwords against these services and will undoubtably gain access to many consumer systems. This allows them to grant access through firewalls and to gain access to wireless networks, security cameras, and any other internal network equipment.

At this point, the company-owned computer is now operating on a compromised network and

stands little chance of not being compromised itself.

Home networks have become complex environments, with potentially many different systems in operation. Examples are gaming consoles, smartphones, network-attached storage (NAS) appliances, audio equipment, exercise equipment, home automation systems, and security systems.

The compromise of any of these systems could pose threats to the company-owned computer and the employee working from home. For example, the Ring video doorbell system had a vulnerability that was identified in 2018 that allowed access to the Wi-Fi password for the home network.

Vulnerable Network Devices
The Internet of Things (IoT) explosion of consumer devices continues to produce insecure and highly vulnerable network devices. These devices are typically running outdated versions of Linux that are never updated and utilize no security best practices. Data is usually sent unencrypted, including passwords or other authentication tokens.

A lightbulb with a network connection could provide a vulnerability where an attacker gains access to a home network. The attacker can then target internal systems including the company-owned computer.

Securely configuring network equipment is difficult even

An attacker can use administrative access to install backdoors to capture keystrokes, dump the contents of memory, and steal files from local storage.

in enterprise environments. Most home users do not have the experience necessary to understand the potential risks of weak security configurations. The home wireless network is a good example: users must select a strong passphrase to secure their networks.

Wireless Passwords

A wireless password needs to be at least eight characters, but it could still be something as simple as the user's last name, their address, or even their phone number. Because most home users are not monitoring their logs, an attacker can simply spray these basic passwords at the remote worker's wireless network until they gain access.

Secure configuration goes beyond just wireless passwords. Many consumer technology platforms require inbound firewall rules. The popular video game Minecraft allows a player to set up their own private server, for example. Parents that configure their firewall to allow their children to host a private Minecraft server may not be aware that this could be used by an attacker to gain access to internal systems. If their children have access to open the connection themselves, the parents may not even be aware of the firewall change.

Password Selection

The selection of passwords for computer systems on the home

network is another aspect of secure configuration that can be a vulnerability. Ransomware attacks prey on both weak passwords and weak authentication for administrative accounts. An employee using BYOD will probably utilize a very weak administrative password for their system. The company systems they access could be very secure, but an attacker may be able to compromise the employee computer to steal passwords and gain access.

An attacker can use administrative access to install backdoors to capture keystrokes, dump the contents of memory, and steal files from local storage. These types of compromises can be devastating for the company: it may not even know how passwords from its systems were leaked.

An attacker may not even need to apply brute force to a weak password if they can get the employee to install the backdoor software themself. Home users tend to search for free software utilities to accomplish basic tasks like editing PDF files or drivers for their computer system.

Attackers have modified these utilities and added their own malicious content and placed them on the internet. The modified utilities get indexed by web-search engines and are now presented to the employee as a solution to their problem. Users unwittingly install the backdoor into their system, and

The firewall can then utilize a virtual private network (VPN) that connects back through the employee's network so that any traffic is encrypted and cannot be intercepted.

the attacker gains access to any company data, including remote-access passwords.

Home networks need to be bypassed using a corporate VPN or managed by organizations to provide adequate security. The organization can provide a managed firewall and wireless access point to the employee to install on the home network. This segregates the network traffic and prevents other devices from communicating with the company computer systems.

The firewall can then utilize a virtual private network (VPN) that connects back through the employee's network so that any traffic is encrypted and cannot be intercepted. The employee computer can then be fully managed just as if it were in the office on the enterprise network.

In short, the basic convention is to treat the home network as an internet connection — not a trusted network.

REMOTE-ACCESS TECHNOLOGY RISKS

Companies had to quickly increase capacity as workers moved out of the office and back to their homes. This included increasing network bandwidth, upgrading VPN hardware, and adding additional remote desktop and Citrix servers to handle the load. Attackers quickly adapted their tactics as these systems increased the

opportunity ("surface area") for password-based attacks.

There may have been a limited number of users who had access to the company VPN before the pandemic. However, the movement of users to their home offices increased the number of username and password combinations that could be tested against these devices. Password-spraying attacks increased dramatically and continue to this day.

Remote access using any type of remote desktop technology like Citrix, Microsoft RDP, or VMware virtual data interface (VDI) are particularly targeted because they provide a desktop on the inside of a network. This allows an attacker to immediately move to targeting internal systems by stealing additional credentials to move laterally through the network.

Because the attacker will be using valid user credentials, these types of compromises are difficult to detect. The motive for these attacks is typically ransomware based, with devastating business impacts.

Dramatic Increase in Vulnerabilities

The number of identified vulnerabilities in remote-access systems increased dramatically in 2020 as attackers adapted to remote working. Vulnerabilities identified in remote-access systems from Cisco, Citrix, F5, SonicWall, and Fortinet could allow an attacker to gain access remotely. All of

Organizations can use sender IP reputation filtering to block known attack addresses. They may want to use geographic blocking as well.

these companies responded with software updates to address the issues that had been identified.

Organizations that were not paying attention to these software updates may have been unknowingly compromised. Attackers are still actively scanning the internet for these vulnerabilities, and organizations will see evidence of these attacks in their firewall logs.

Multi-factor authentication should be considered a mandatory requirement for remote access. This will prevent the success of the password-spraying attempts. However, organizations still need to monitor their logs to identify password-spraying attacks and take defensive actions. This could include network rate limiting to slow the attempts.

Organizations can use sender IP reputation filtering to block known attack addresses. They may want to use geographic blocking as well. The important point is to monitor and react to changes in attack vectors rather than simply trust that the technology alone will provide adequate defense.

CONSUMER VPN ISSUES

A growing issue with remote access is the use of consumer virtual private network solutions. These products advertise security and privacy for home users. The problem is that the users do not realize that they just changed who has access to their usage data from

their internet service provider (ISP) to their VPN provider.

That can be a problem, because not all VPN providers are equally interested in privacy and security. Remote users are then connecting to company resources through these untrusted networks, thus creating the potential for interception or data leakage. Also, many VPNs offer connections through foreign countries, which could impact organizational compliance as well.

The effectiveness of defending remote-access infrastructure through log activity monitoring is greatly reduced when employees use consumer VPN solutions. The metadata that would help identify the authenticity of a user authentication (like geographic location) is missing. Attackers are aware of this and utilize these consumer VPNs to hide their activity.

The IP addresses used by consumer VPNs are often identified as threats due to the amount of malicious activity conducted over these networks. Information security teams are not able to separate the attackers from legitimate remote-access users.

There is no security benefit gained by using a commercial VPN when connecting remotely to company resources. Organizations should utilize their own VPN solutions and block access from any anonymous

The monoculture of most businesses using the same cloud platform allows for economy of scale for attackers. They can target a single technology platform and then target most businesses with a single attack.

source. The listings of these IP sources change frequently and will require a subscription to a threat intelligence or IP reputation feed.

The cultural impact of blocking commercial VPNs can be difficult because of the way VPNs are marketed to consumers. However, this problem can be addressed by focusing on the fact that permitting anonymous access to any company resources is a bad practice.

CLOUD SECURITY ISSUES

The movement to the cloud was well underway before the COVID-19 pandemic. However, the rapid migration to a remote workforce accelerated this movement.

In just a few short years, Microsoft 365 has become the dominant office collaboration suite used by the majority of companies. This has had both positive and negative impacts to information security risk. The monoculture of most businesses using the same cloud platform allows for economy of scale for attackers. They can target a single technology platform and then target most businesses with a single attack.

The volume of data stored in Microsoft 365 makes it a prime target for attackers as well. They can get access to email as well as files through SharePoint and OneDrive. They get access to logs of Microsoft Teams messages and, potentially, phone calls and voicemails.

An administrative account on Microsoft 365 would allow the attacker to modify security settings, including workstation software deployment, through Endpoint Configuration Manager and antivirus settings through Microsoft Defender. The combination of being a one-stop shop for data access, along with the popularity of the platform, makes Microsoft 365 a primary target for attackers.

Microsoft has started implemented multi-factor authentication for new Microsoft 365 accounts as a primary defensive control. Attackers have been using password-spray attacks aggressively against Microsoft 365 accounts in the past year. Surprisingly, Microsoft has not addressed complex passwords in Microsoft 365. It requires only an eight-character password, making multi-factor a mandatory requirement for secure access.

Disabling Older Protocols

A default installation of Microsoft 365 allows attackers to bypass multi-factor authentication by using older email protocols that do not support stronger authentication measures. To prevent these attacks, the older protocols should be disabled during configuration of Microsoft 365.

The primary benefit of using cloud-based collaboration tools is that they easily share data. This is great for companies looking to increase efficiencies, especially when working remotely. It also

The overriding design concept for any of these security solutions is to maintain visibility and control into the networks, devices, and cloud solutions used by remote workers. The approach to securing remote workers is to extend the same types of security controls in place on the enterprise network to the home network.

means that it is very easy for an employee to accidentally leak data by inadvertently sharing something as public (for example, within Microsoft 365 or collaboration tools) — or sharing with the wrong individuals.

The default configuration of Microsoft 365 allows wide-open sharing with no regard for security controls. The platform does provide very granular security controls with a variety of options for preventing data leakage including data loss prevention (DLP) tools. Before deploying Microsoft 365, organizations need to review the security capabilities of controls and ensure their appropriate configuration.

CONCLUSION

There is no silver bullet for providing secure remote-access solutions for home-based workers. However, there are a variety of approaches and solutions that can be used to manage the risk to appropriate levels.

The overriding design concept for any of these security solutions is to maintain visibility and control into the networks, devices, and cloud solutions used by remote workers. The approach to securing remote workers is to extend the same types of security controls in place on the enterprise network to the home network.

Organizations that jump too quickly and use consumer-grade

technologies that rely on employee configuration are accepting critical risks to their business that could be managed with simple solutions and a plan.

In summary, here are nine recommendations for protecting the organization and its employees:

1. Provide company owned equip- ment for remote workers where possible
   - computers
   - firewalls and routers
   - Wi-Fi access
2. Utilize strong mobile device management controls for any personal or company-owned devices.
3. Utilize corporate VPN solutions to isolate business traffic from personal traffic.
4. Utilize multi-factor authentica- tion for all websites and remote access.
5. Harden and secure cloud-based productivity systems like Office 365.
6. Monitor security logs from any cloud-based system and onsite remote-access systems.
7. Restrict usage of consumer VPNs that anonymize traffic to company resources.
8. Provide frequent training on social engineering to all employ- ees.
9. Require alternative communi- cations channels for approving financial operations like wire transfers, direct deposit, and vendor payment changes.

Joseph Granneman

jgranneman@illumination.io

Joseph Granneman is CEO of illumination.io in Cherry Valley, Illinois. He founded the cybersecurity company in 2013 following more than 20 years of experience as an executive IT leader in healthcare and financial trading institutions. He is an expert in penetration testing in the banking, manufacturing, and healthcare vertical markets; incident response; and forensic analysis as well as regulatory compliance with HIPAA, PCI, and NIST security frameworks. He has worked closely with the FBI and Secret Service on behalf of his clients who have been victims of cybercrime. Mr. Granneman has written articles for Information Security and CIO/CSO magazine and publishes online with TechTarget at http://searchsecurity.techtarget.com. He is an adjunct professor of IT strategy for the MBA program at Northern Illinois University's College of Business in De Kalb, where he also received an MBA in 2011. He is involved in developing as proposal for secure healthcare data exchange for the state of Illinois. In addition, he helped develop security standards for emergency medical responders as part of serving on the Certification Commission for Health Information Technology Security Working Group. Mr. Granneman received a BS from Millikin University, Decatur, Illinois, in 1993 and also holds the CISSP (certified information systems security professional) credential. His last article for this journal was "The Business Guide to Improving Information Security," in the Fall 2018 issue (vol. 36, no. 3).