



The BAUMAN LETTER

— YOUR GUIDE TO ROGUE FREEDOM & BOLD PROSPERITY —

Privacy: Your Most Valuable Asset

THE message arrived in the early hours of the morning.

He was in the habit of all-nighters, so that was fine ... until he read it.

Someone had just changed the password on his email account.

That was the last email he received. A few seconds later, he got an “incorrect login” message ... because of the new password.

Then he was locked out of his own PC. Someone had changed that password as well, remotely.

This was one instance where insomnia was a blessing, albeit a minor one.

Given how quickly the hackers accessed and drained his financial accounts, sleeping would have left him *completely* broke.

He spent the next few hours frantically calling banks and brokerages, trying to protect what he could.

Thanks to his sleep habits, he only lost tens of millions of dollars.

At least he could still pay his rent.

The victim of this true story was tech-savvy enough to trade in bitcoin when it was still a new thing.

Most of his losses were from bitcoins drained from

his online wallet and from “secure” storage on his PC.

In this instance, the hacker’s scam took advantage of systemic weaknesses. It wasn’t something the victim did, like click on a “phishing” email.

Instead, it was something he *didn’t* do.

He took his information environment for granted. He addressed risks he knew about ... but he didn’t ensure that he found out about new risks quickly.

He found out about the “two-factor text message” scam as it was happening ... to him.

Imagine you treated your investments that way ... resting on your laurels, neglecting to cultivate new sources of information (such as one of my colleagues’ services).

You’d miss out on big opportunities ... because you found out about them too late.

One of my favorite financial quotes is from an adviser of mine: “Remember, focusing on ‘downside’ risk (not losing money) is more important to long-term financial success than swinging for the fences on your next trade. This is how the ultrawealthy stay wealthy.”

You, no doubt, apply that insight in your investing.

But do you apply it to your information privacy — and to the serious threats it can pose to your wealth?

INSIDE THIS ISSUE

10 | **Cybersecurity: It’s Getting a Little Better All the Time**
By Brad Deflin

12 | **Guanxi (关系) Is Corruption in Any Language**
By Bob Bauman JD

13 | **The Perils of Ignoring Debt**
By Ted Bauman

The Four Horsemen of Privacy

“Privacy” is a state of *personal control* over information about you and of access to you.

“Digital information security” is the technique you must use to secure your privacy in the modern age.

There are four types of privacy, which are essentially *assets*. And just like any other asset, they must be protected just as you would protect gold, jewelry, your bank accounts ... anything of value:

- **Financial privacy** is important for the avoidance of fraud, including identity theft. But that’s not all. Information about credit card purchases, for instance, can reveal a great deal about your preferences, places you’ve visited, your contacts, products you use (such as medications), your activities and habits, etc. Financial privacy also includes privacy over bank accounts and other financial arrangements.

- **Digital privacy** is the ability to control what information about you is revealed on the Internet, when communicating via email, phone or other electronic means, as well as storage of private digital data. It involves who has access to such information and for what purposes that information may or may not be used.

For example, as you know, many of the websites you visit collect, store and share personally

ABOUT TED BAUMAN

Ted Bauman is the editor of the Plan B Club, a blueprint to help protect your wealth and escape excessive taxation, regulations and wealth confiscation in America. He is also the editor of *The Bauman Letter*, a newsletter that’s brimming with up-to-the-minute asset protection strategies, tips on buying and investing in real estate abroad, and retirement and residency secrets in American-friendly countries around the globe. Ted has been published in a variety of international journals, including the *Journal of Microfinance*, *Small Enterprise Development* and *Environment and Urbanization*. Email Ted your thoughts and questions at baumanletter@banyanhill.com

identifiable information about you. Email and phone conversations shouldn’t be accessed, read, stored or forwarded by third parties without your consent.

- **Medical privacy** is governed by federal law that allows you to withhold your medical records and other information from others. This helps you control its impact on insurance coverage or employment, in order to avoid embarrassment caused by revealing medical conditions or treatments. Medical information can also reveal other aspects of one’s personal life, such as sexual preferences or proclivity.

- **Political privacy** has been a concern since voting systems emerged in ancient times. The secret ballot helps to ensure that you can’t be coerced into voting in certain ways, since you can vote in the privacy and security of the voting booth. But there is another aspect of political privacy: preventing your private views from being broadcast to the world, as happened, for example, to Clinton adviser John Podesta in the 2016 election when his emails were hacked.

The Threat

Make no mistake, your privacy in all these areas is under constant threat. Here are the main ones:

INTERNET TRACKING

Most websites install “cookie” software agents that track your browsing habits and personal data. So do advertising networks, marketers and other data profiteers. They depend on cookies to learn more about who you are — and what you may be interested in buying.

Ten years ago, if you opened NYTimes.com in your browser, you’d get a cookie from *The New York Times*, maybe a couple, and that would be it. Today, you get 50 or more cookies from all sorts of third-party ad servers, data brokers and trackers. They build up a big profile about your browsing history — and, thus, about you.

CLOUD STORAGE

Whether you use a Web-based email service, keep files in Google Drive or upload photos to Dropbox, everything you write, upload or post is stored on a

server somewhere that belongs to the online service, not to you.

Because of outdated federal rules, this cloud-based data is vulnerable to a massive privacy loophole: Your data does not have the same Fourth Amendment protections that it would have if it were stored in a desk drawer, or even your desktop computer.

Current law treats data stored on a server for more than 180 days as “abandoned.” To make matters worse, the definition of such data is vague enough to cover not just email messages, but other kinds of data stored on third-party servers.

There was a vestige of a time when servers held data only briefly before passing it off to a local computer. But now that so much data resides on servers owned by cloud-based services, and so many people keep content in the cloud for years, a lot of long-stored files that people haven’t abandoned are fair game for government or courts. Law-enforcement interests have consistently defeated attempts to update this situation.

LOCATION TRACKING

Location data, such as your cellphone signal or GPS device, allow others to know exactly where you are at any given time. Location data you post to social networking sites are revealing sources, too. That includes what’s known as “EXIF data” that’s embedded in digital photographs you post to Facebook, for example.

Imagine law enforcement officials, your employer or your ex-spouse’s private detective using location data to watch you. As with cloud-based data, the legal requirements for obtaining location data from your mobile service provider are not very stringent.

DATABASES

Posting and tagging photos online helps build facial recognition databases that make escaping notice increasingly difficult for anyone.

Facebook, for example, uses the tags associated with user photos to build ever-more detailed “faceprints” of what you and your friends look like from every angle. If you share your photos with “friends of friends,” your pictures can be viewed by over 100,000 people on average.

Even worse, when Facebook sells user data to third parties, photo data may be included. Nobody knows how well that data is protected once Facebook sells it. The government also gathers Facebook data for purposes as varied as citizenship applications, criminal cases and security checks — including all photos you’ve been tagged in.

Google and Apple have facial-recognition technology built into some of their applications, too. That means someone can take a photo of you and then track you down based on other identified photos of you that may have been posted on the Web.

Advances in surveillance technology, such as drones and super high-resolution cameras, will make identifying individuals in public places easier than ever — especially if the entity doing the surveillance has a facial-recognition database to consult.

GOVERNMENT SPYING

A 2013 Presidential Policy Directive concerning cybersecurity lists “critical” U.S. business sectors whose employees and correspondence may be subject to monitoring. The definition is broad, and includes financial institutions, utilities and transportation companies.

Anyone who works for or does business with such companies may expect to have the contents of their communications with them surveilled.

Then there is the invasive dragnet surveillance conducted by the NSA and other government agencies in the “war on terror.” There, too, you can easily end up caught in the government’s data fishing expeditions.

But the most egregious misuse of surveillance technology happens at the state and local levels.

Ever since 9/11, the federal government has encouraged state and local law enforcement agencies to acquire and use sophisticated technologies originally developed in the urban warfare zones of Iraq.

These include “stingrays,” which mimic cellphone towers and capture your unencrypted communications; aerial camera surveillance using light aircraft and balloons, which can track the movements of individuals over many hours; facial recognition technology; and “predictive policing” algorithms ... otherwise known as “pre-crime” programs.

Privacy Is Freedom

Despite these threats to our critical privacy assets, some people still think worrying about privacy is much ado about nothing. The horse is out the barn door, so why worry now? Besides, if you haven't got anything to hide...

This is *dead wrong*, in my view. Here's why:

- **Data is the single most valuable commodity in the world today, and you produce it ... without compensation.** As *The Economist* recently put it, data is the new oil. We get access to things like Google and Facebook because they harvest and sell our data to advertisers and others who can profit from it, leaving us with reduced privacy. But is access to a monopolistic search engine and a cheesy social media platform worth that trade-off?

- **Data-based manipulation interferes with your free will.** We like to think of ourselves as free, independent thinkers who make our own choices. But the reality is that we are constantly bombarded with manipulative messages that shape our behavior in subtle ways. Think about it ... would you make other choices if you weren't constantly bombarded with targeted advertisements and other data-based manipulation?

- **When others know too much about you, it limits your freedom to act.** Under rules recently passed by Congress, your Internet service provider can track everything you do on the Internet and sell that information for profit. Think about it ... does your pattern of Internet usage expose you to risks, like blackmail or political harassment? I know mine does. It's not about questionable content, either. If someone wanted to discredit you, they could publish selective details of your browsing history to make you look like some kind of dangerous radical ... or worse. Knowing that, will you — can you — continue to use the Internet freely?

- **If we don't push back, things will get steadily worse.** I've said this so many times that you could call it "Bauman's First Law of Privacy": Any technology that can be used to invade our privacy will be used to invade our privacy. Snoops and

their enablers always find a way to rationalize new abuses of our rights, and as they do, the public's memory or the days of true privacy fade ... making new violations easier as time goes by.

- **Privacy is a basic human right.** When it is abused by others for their gain and at your expense, you are essentially accepting a violation that you would never accept in physical form — such as theft, violence against your person or violation of your right to free speech.

I'm not the only one who feels this way. A recent article in *The Week* observed that:

While battling against federal surveillance has a libertarian streak to it, many Americans are similarly worried about the injustices inherent in such techniques. A majority of Americans disapprove of U.S. collection of telephone and Internet data as part of counterterrorism efforts. Seventy-four percent of voters said they shouldn't have to give up privacy and freedom in exchange for safety, and over a quarter said they've changed their technological habits following the Snowden leaks.

The question is ... what are we going to do about it?

Forget politicians. In a recent podcast, I argued that there is no coalition in Congress to stop the erosion of our privacy rights. Democrats are afraid of being "soft" on security — and often hold quite hawkish views anyway — whilst Republicans generally support the intelligence services at the expense of our own rights. Individual legislators like Rep. Justin Amash (R-Mich.) and Sen. Ron Wyden (D-Ore.) may have strong views about individual liberties and privacy, but they are a small minority.

The Holy Trinity of Electronic Freedom

That leaves you ... and the rapidly expanding market for privacy-enhancing technology. Just consider some of the recent advances on this front:

- **Unhackable methods of digital communication are increasingly available to everyone.** Apps like

Signal allow users to send and receive several types of information, including voice calls, in a way that is impossible to decrypt.

- **Cloud storage companies are competing to provide unhackable data storage.** For example, the Swiss provider I use, SecureSafe, offers a service in which data is encrypted as it is transmitted to its cloud servers, and encrypted again as it is stored. The company cannot read any of the data its users store on its servers ... and neither can anyone else, search warrant or not.

- **Publicity about hacking incidents is forcing Internet of Things companies to adapt their technology.** For example, owners of Internet-connected gadgets like home cameras are increasingly demanding the ability to set their own passwords, preventing external hacking — such as the incident in 2015 that hijacked tens of thousands of cameras and brought down part of the U.S. Internet. That is forcing manufacturers to compete to produce low-cost network interface chips that accommodate this demand.

- **Companies like Google are forcing websites to adopt HTTPS encryption.** HTTPS is an automatic protocol that encrypts data flowing between you and a website — say, your online brokerage. Google and other companies are increasingly using their dominance in online search to reward companies that adopt this protocol for their own websites with better search results.

- **Digital security systems previously limited to corporate environments are becoming available to individual and small-business users.** As Brad Deflin writes later in this issue, companies are developing mass-based rapid-response platforms that prevent most forms of hacking.

These developments share three things ... what I call the “Holy Trinity” of digital security:

1. **Encryption** is so easy to use that anyone can adopt it without fuss. Very little of our personal communication and data needs to be readable by third parties ... so we should choose to make it unreadable through strong encryption.

2. **Risks** are identified automatically by all players in the digital information chain working cooperatively ... even if they aren't doing it consciously.

3. **Response time** is shortening so that threats can be eliminated before they snowball. Viruses, for example, can't propagate if users have instantly updated threat protection software installed. That's why we haven't seen any big outbreaks in the last few years.

Be Your Own Savior

This “Holy Trinity” is essentially the key *characteristics* of a secure information environment.

Fortunately, consumer demand for digital security is leading market participants — hardware and software manufacturers, websites and big tech companies — to make their part of the digital information environment more secure by adopting the “Holy Trinity” as their guiding principle.

But the key element in all of this is **you**.

If you don't adopt these principles, too, they might as well as not exist. It's up to you to choose to:

- Use encryption to protect your data, both in static (communication) and dynamic (storage) form.
- Minimize the data you reveal when you use the Internet.
- Find and use real-time protection services that neutralize threats as soon as they emerge.

Fortunately, these things are easily achievable, thanks to the market forces driving the pro-privacy developments I listed above.

Encrypt It!

It all starts with encryption ... scrambling information so that you, and only you, can read it.

I routinely digitize my important personal documents and artifacts and store them in a “digital safe” as well as on a secure server in Switzerland.

You may think I'm taking great risks doing this. It's bad enough that I'm turning my passports and other important papers into digital form where they could be hacked, but I'm also storing them on a server

I've never seen, in a foreign country, run by people I've never met. Right?

Not at all. That's because everything on my computer and in the cloud is *encrypted*.

NSA whistleblower Edward Snowden — who knows a thing or two about encryption — maintains: “Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.” And if the directors of the FBI and the NSA don't like encryption — *they hate it* — it must be worth it.

Encryption is used at many different stages in the handling of digital information. The two most important are when information is in *storage* and in *transit* — what I call *static* and *dynamic* information environments. Encryption is the bedrock of information security.

To protect my digital assets, I use a combination of file encryption, encrypted communications and encrypted cloud storage. So should you.

All three work by using special software to scramble digital information into seemingly random sequences of letters, digits and symbols. It can be unscrambled only with a special “key” — a password or passphrase.

FILE ENCRYPTION

There are two types of file encryption for your computer, and they can even be used together:

1. Full-disk encryption protects your entire computer or phone in case they are stolen or breached. It works on any device. The goal of disk encryption is to prevent someone who gains access to your device — such as a lost or stolen laptop or phone — from reading the files stored on it. For full-disk encryption, I recommend DiskCryptor. It uses 256-bit encryption, and it's managed by the Electronic Frontier Foundation, one of the best outfits around dedicated to digital security. It's easy to set up and use.

2. File encryption does the same thing, but on a file-by-file basis. Even if an encrypted computer is hacked, individually encrypted files are invulnerable. The goal is to lock down your most sensitive files — whether they're photos, financial documents, personal backups or anything else — and keep them

locked down so only you have the key. Most freely available file encryptors work just fine.

Your cellphone is a storage device too. Typically, cellphones do not contain files, but rather links to files stored in the cloud. For this reason, smartphone encryption is generally based on encryption of the entire device rather than its storage drive or individual files.

For example, all Apple devices from iPhone 6 onward are 256-bit encrypted when you choose to use a master password.

Everything on the phone — contacts, emails, texts, photos and so on — is only accessible via the password you set for it. Even Apple cannot read it. The same goes for most Android phones, which use Google software.

VIRTUAL PRIVATE NETWORKS

File encryption addresses risks facing static data — data that's stored on your machine. But what about dynamic environments ... when data is moving between places?

Truly secure communication is only possible by using a virtual private network (VPN).

A VPN creates an encrypted private network for you across the Internet. It enables a computer or network-enabled smartphone to send and receive data as if they were directly connected (“tunneled”) to whatever is on the other end, such as websites you visit. The walls of this digital tunnel are rock-solid, protected by the same encryption technology that protects the files on your hard disk.

Within a VPN, the IP addresses of any device using it are hidden from outsiders, so nobody knows where you really are, physically. As I'm working on this report, the Internet thinks I'm in Iceland.

That means that even though the VPN is making use of the public Internet, everything is completely invisible to those without the right VPN credentials — sites you visit, where you are, and information you send and receive.

VPNs are absolutely critical when using free public Wi-Fi, especially in places like airports. Without it, everything you do whilst logged in to the Wi-Fi network is *en claire*. But with a VPN enabled, you're safe and sound.

Setting up a VPN on your computer or phone involves installing a piece of software that converts your Internet traffic into a password-protected, encrypted form. You use the same browser and email program you normally do.

In the past, I've been ambivalent about which VPN to use. They're all pretty good, as long as they're not free — if they are, you can't trust them not to sell your data that crosses their servers.

But after Congress rescinded the Obama administration's ban on Internet service providers selling your browsing history, I looked further into the VPN world and decided to use and recommend Nord VPN. It costs \$69 a year, but covers up to five separate computers and cellphones.

- **Pros:** Easy to set up and use; works on Windows, Mac, iOS or Linux; a wide range of server types with varying levels of encryption; uses 256-bit AES for encryption, RSA-2048 for handshaking and SHA-2 for authentication; a strict no-logs policy, so nothing you do is recorded anywhere; and it's located outside the U.S.

- **Cons:** Can be a little slow to resolve new websites when you first visit.

The next step up is to use the Tor Browser. Tor has its own browser interface that allows most users to use the web entirely anonymously.

Tor is similar to a VPN, but it's free. Tor is also open-source and operates through distributed computers rather than a central server, which means it can't be "hacked" or invaded at any crucial point. Tor has become much easier to use and more secure since the Snowden revelations emerged, but it remains a more complex technology than a simple VPN service.

SECURE CLOUD STORAGE

Storing your data on the cloud seems counterintuitive.

On one hand, as I mentioned earlier, since the government can access your cloud data with the right court order or subpoena, it seems like an insecure thing to do.

On the other, however, cloud storage providers are increasingly adopting encryption systems, which

means they can't read or share your data with anyone even if they wanted to. On top of that, if you store the encrypted version of your files on a cloud server, you control access to them, even if the cloud service is prepared to hand them over.

I have accounts with Dropbox, Microsoft OneDrive, Google Photos and Amazon Music. Anything I store on them that is sensitive in any way is encrypted by me using my passphrase, before it goes to their servers.

But for extremely sensitive stuff — including my password vault — I have an account with a group called SecureSafe out of Zurich. Besides the fact that they're located based in a privacy-friendly jurisdiction, their servers are located in a nuclear bomb-proof cave deep inside an Alpine mountain.

I find their system easy to use, fast and reliable.

Best of all, they allow me to designate certain individuals as my digital "heirs," so they can access my data with private credentials I've given them if I die or am otherwise unable to do so. That's a significant bonus over standard cloud storage providers, which often ask for court orders to open your files, even for relatives.

A Note on Passwords

Passwords and passphrases are critical to your information security efforts, especially encryption.

They are the single most important thing protecting your encrypted data.

It's important to understand how they work and how to develop a good one.

Password strength is measured in terms of "entropy." Entropy is measured in bits. Bits determine how many guesses it would take to crack the password.

For instance, a single six-digit password in 32-bit encryption would take 4,267,967,296 guesses to crack. It would take approximately a month and a half for an NSA supercomputer to try all those guesses.

But a seven-word 128-bit passphrase like "waltzed assemble maverick tonsil subsumes gunner submarine" would require 165,874,258,366,850,931,470,183,446,872,064 guesses. At 1 trillion guesses

per second, it would take 27 million years for the fastest supercomputer to crack this.

That's why *passphrases* are the preferred approach to true digital security these days — not individual *passwords*. For the important things, you want to use a passphrase.

Here's how to generate totally random passphrases.

You roll a six-sided die five times, and write down the numbers that come up.

If you roll the number two, then four, then four again, then six, then three, look up 24463 in the Diceware word list (<http://world.std.com/~reinhold/dicewarewordlist.pdf>). There you'll find the word "epic." That would be the first word in your passphrase.

Repeat until you have a seven-word passphrase ... one that nobody could break in 27 million years.

Data Minimization

With Chrome or Firefox, you can customize for privacy to your heart's content.

For example, on my personal Google Chrome installation, I use the following "extensions," which are all free and can be found on Chrome's Web store.

By using them, I put serious obstacles in the way of data trackers, adbots and others trying to harvest and sell information about me:

- **uBlock Origin**, which prevents most tracking cookies and ads.
- **Collusion**, which shows what information websites silently send to and receive from other websites that I never directly visit.
- **HTTPS Everywhere**, which encrypts my web traffic on most sites.
- **IBA Opt-out**, which prevents Google and other sites from tracking my browsing habits for advertising purposes.

Combined, these little tweaks make me almost impossible to track. They are one of the simplest and most effective things you can do to reduce your Internet footprint.

But just to be safe, I also disable almost all the

tracking features on Google, using <https://myaccount.google.com/>.

I also make sure I log out of Facebook, Google (including Gmail and YouTube), LinkedIn and so on when I'm browsing. That's because if you're logged in, those companies will be able to track most sites you visit for marketing purposes.

Finally, for my searches, I use DuckDuckGo.com, a free search engine that doesn't track your usage or anything else.

The Ultimate Real-Time Protection

Perhaps the single most effective thing you can do to protect your digital information privacy is to turn it over to someone else.

It sounds paradoxical. But think about it: In large corporate environments where thousands of individual workstations and laptops must be protected from all sorts of evolving threats, it would be suicidal to rely on each user to keep themselves safe.

Instead, the corporate best practice is to monitor each individual device connected to its networks — computers, cellphones, tablets, even smart devices like whiteboards — from a central security center. Digital security is rolled out as a service to the entire corporate community.

It isn't something individual users have to worry about unduly. It just happens.

That's exactly what some enterprising companies have started to do ... but for families and small businesses. Here's how it works.

Let's say you have four computers — two PCs and two laptops — along with four smartphones in your family.

A digital security company can install a firewall on your home network that is constantly updated with details of evolving threats. Besides protecting you from the old-fashioned stuff — like remote hacking attempts — this firewall also protects against phishing and malicious websites using databases that are updated in real time ... just as corporate IT departments do.

In addition, each computer and smartphone has

an app installed that scans for security weakness, updates patches and other vulnerabilities, and reports them back to the security provider. When a serious vulnerability is detected, you can arrange to have the provider notify you by screen pop-up, email or even just fix it without alerting you.

Finally, the security provider provides a VPN and other protections for roaming devices like smartphones and laptops, which protect you against insecure public Wi-Fi networks when you're on the road.

The same system can work for any small business.

The beauty of such a system is that by providing individual-level service to many users at once, the security company can achieve the same economies of scale that allow large corporations to invest in serious, heavyweight digital defense systems that cover their own employees. You get the same benefits that say, IBM, Apple or Google would get for its own workforce ... at a small monthly subscription cost.

To me, this is one of the most promising developments in modern digital information security.

It can provide world-class protection to anyone, at a fraction of the cost of traditional standalone systems like anti-virus software and firewalls ... which are nowhere near as effective as real-time monitoring.

Conclusion: Don't Go IT Alone

The fellow I wrote about at the beginning of this report lost millions because he was behind the curve when it came to the latest asset protection techniques ... digital asset protection, that is. He wasn't aware of a rapidly evolving form of hacking, and he paid the price.

Two-factor authentication (2FA) is a simple technique to enhance password protection.

For every sensitive login you may have ... banks ... brokerage accounts ... your cloud storage account ... you must do two things to login.

First, you must enter your password or passphrase.

Second, you must receive a separate random code and enter it in the login process as well. This code

must be sent to a separate destination, like your cellphone or email address, that only you can access. It ensures that the person trying to log in with your password is actually you.

But there is one caveat: Do NOT use text messages for 2FA. The fellow I described at the beginning of this report did, and it ruined him. Here's how.

The hackers gathered as much information about the victim as they could — his ID number, names of relatives and pets, date of birth, address and so on.ere'

Then they called his cellphone company and used this "personal identifying information" to convince a minimum-wage call center operator to transfer his cell service to another mobile provider.

Once that was done, the hackers had all his cell calls and text messages diverted to a Google Voice account they had set up. Even though the victim still had his cellphone in his physical possession and text messages went to his number as part of a 2FA verification process, the texts were diverted to the hackers. They used them to change the passwords on all his logins, and then to drain his financial accounts.

Using his email as 2FA would take the mobile company out of the equation and force any attempts to change his email password to come to him at his email address, where he could stop them.

It's little things these that make keeping informed about digital privacy ... and having reliable sources of information and service providers that stay on top of these matters ... so crucial.

So take care of the little things ... and the big things will take care of themselves.

Contacts

A firm that provides excellent real-time digital security services is Total Digital Security, based in Florida. I have tested their products and appeared on several panel discussions with their CEO, Brad Deflin. I recommend them highly.

301 Clematis Street, Suite 3000

West Palm Beach, FL 33401

877-643-6391

info@totaldigitalsecurity.com

<https://www.totaldigitalsecurity.com/> ■

Cybersecurity: It's Getting a Little Better All the Time

BY BRAD DEFLIN

THE Beatles once sang: "I've got to admit it's getting better. A little better all the time."

You might not read about it in the headlines, but cybersecurity threat protection technology is getting better all the time.



Over the past few years, a record amount of new capital investment has flowed into the cybersecurity industry. Smart investors are fueling innovation as never before.

These investors target companies that seek to take proven cybersecurity techniques used in corporate environments and make them available to individual households and small-business subscribers.

That means making the technology easier to use, effective and affordable for almost anyone.

In other words, it means making the technology better all the time.

Evolving Cybersecurity Device Protection

A fitting example of such progress in mass-market cybersecurity is device protection software.

Device protection software defends your personal computers and smartphones from ransomware, viruses and other malware that can cause you and your devices permanent harm. But it does it in a very different way to the old anti-virus programs.

Indeed, the old days of retail anti-virus solutions are over. They just aren't useful in the threat environment we have at hand today.

They're too slow to respond. By the time the threat is identified and the definition database is updated, your computer may already be infected.

But next-generation cybersecurity software is plenty fast enough, and it's available to anyone ... not just large corporations with big budgets and IT departments.

Innovation in cybersecurity for personal technology has advanced. The key innovation is that, just as operating systems like Windows have become

RMM is truly "set it and forget it." Your device protection software is constantly optimized using the latest intelligence and defenses available at any given time.

services rather than stand-alone products, sold once and then upgraded a year later, cybersecurity is now a service that evolves constantly.

That's why something called "RMM" — remote monitoring and management — is no longer just for big companies. It's now available for your Mac, Windows and Android devices.

RMM is "smart" protection that operates in real-time with pre-emptive defenses that are adjusted and updated automatically, with no user input required. Within 60 seconds of a new threat appearing on the Internet, your device is updated and protected, 24/7/365.

RMM has been common in corporate environments for some time now. A dedicated team in the IT department scans for and identifies emerging threats. When one is detected, it sends out an instant patch to networked devices, protecting them.

The patch, however, isn't always a direct "fix" of the vulnerability, like those that Microsoft issues frequently for Windows.

Instead, the initial protection might just involve disabling the functionality that contains the vulnerability.

For example, certain types of software "scripts" that run on Web pages might be disabled to prevent them from being exploited.

When the scripts are repaired, they are re-enabled ... all without you having to do anything.

RMM can do other things, too:

- Install new or updated software remotely, including patches, updates and configuration changes.
- Detect new devices and automatically install the RMM agent and configure the device.
- Observe the behavior of a linked device and its software for performance and diagnostic tasks.

- Provide alerts, reports and monitoring dashboards.

Cybersecurity Made Easy

RMM is truly "set it and forget it." Your device protection software is constantly optimized using the latest intelligence and defenses available at any given time.

This device protection software works so well that not a single customer of mine has decided against renewing their annual subscription for the service since we started almost four years ago.

The device protection software we recommend as best-in-class works on iMacs, MacBooks, all Windows machines and Android devices.

We have many years of increasing cyber-related risks ahead, but the protective technology is getting better, a little better all the time. Use it and see. ■

Brad Deflin is a seasoned business executive with success at both the large corporate level, and in the pioneering of start-up companies. Brad co-founded Total Digital Security. Contact Brad at Brad@TotalDigitalSecurity.com.

All international and domestic rights reserved, protected by copyright laws of the United States and international treaties. No part of this publication may be reproduced in any form, printed or electronic or on the worldwide web, without written permission from the publisher, Banyan Hill Publishing, P.O. Box 8378, Delray Beach, FL 33482 USA.

Legal Notice: This work is based on what we've learned as financial journalists. It may contain errors and you should not base investment decisions solely on what you read here. It's your money and your responsibility. Nothing herein should be considered personalized investment advice. Although our employees may answer general customer service questions, they are not licensed to address your particular investment situation. Our track record is based on hypothetical results and may not reflect the same results as actual trades. Likewise, past performance is no guarantee of future returns. Certain investments such as futures, options, and currency trading carry large potential rewards but also large potential risk. Don't trade in these markets with money you can't afford to lose. Banyan Hill Publishing expressly forbids its writers from having a financial interest in their own securities or commodities recommendations to readers. Such recommendations may be traded, however, by other editors, Banyan Hill Publishing, its affiliated entities, employees, and agents, but only after waiting 24 hours after an internet broadcast or 72 hours after a publication only circulated through the mail.

(c) 2017 Banyan Hill Publishing. All Rights Reserved. Protected by copyright laws of the United States and international treaties. This Newsletter may only be used pursuant to the subscription agreement. Any reproduction, copying, or redistribution, (electronic or otherwise) in whole or in part, is strictly prohibited without the express written permission of Banyan Hill Publishing, P.O. Box 8378, Delray Beach, FL 33482 USA.

Guanxi (关系) Is Corruption in Any Language

BY BOB BAUMAN JD

As a member of the U.S. House of Representatives from Maryland, by chance I was seated in a group at a White House luncheon table along with President Jimmy Carter, who had campaigned for my defeat.



Feeling feisty, I reminded the president of his quote that I was a “good example of all that is wrong with the Republican Party.” Carter smiled his famous toothy smile and said: “Well, Congressman Bauman, wasn’t I prescient?”

In the April edition of *The Bauman Letter*, I was indeed prescient.

My topic was the need to end a fundamentally corrupt but legal U.S. immigration program: the “employment-based preference immigrant investor program.” Also known as the EB-5 visa, it grants U.S. citizenship in exchange for investments of \$500,000 to \$1 million.

The EB-5 visa is called the “Golden Visa” by its major beneficiaries: American real estate promoters obtaining millions from wealthy foreigners — especially from Chinese willing to pay for U.S. citizenship.

Two events in the news have made the abolition of the EB-5 visa timely.

First, despite widespread demands for repeal — or drastic reform — the U.S. Congress extended EB5’s existence until October 1. Without debate, the extension was buried in the 1,665 pages of the Consolidated Appropriations Act of 2017, a Capitol Hill backroom deal that avoided another federal government shutdown.

The second event underscoring the need to end EB-5 occurred 6,933 miles away from Washington, in the ballroom of the Ritz-Carlton Hotel in Beijing.

On May 5, Nicole Kushner Meyer, the sister of White House senior adviser Jared Kushner, lauded the EB-5 visa as the best way attendees could buy U.S. citizenship. Just invest hundreds of thousands of dollars

in a New Jersey luxury apartment complex owned by the Kushners, she advised.

Listeners were reminded that Ms. Meyer’s brother, Jared Kushner, is a top official in his father-in-law’s White House, where he serves as a crucial diplomatic channel between Beijing and the Trump administration.

The Chinese have a word for official corruption: *guanxi* (关系, pronounced *fūbài*). Bribery and insider dealing is rampant in China, so Ms. Meyer’s presentation in Beijing was well-understood: Get on the inside with a Kushner deal.

Corruption is defined as the misuse of entrusted power for personal gain. It describes decisions that politicians and public officials make as motivated by self-interest, rather than by public interest. The EB-5’s visa history is marked with corrupt political influence and outright fraud.

The U.S. Supreme Court is currently considering a case, *Kokesh v. SEC*, in which an EB-5-financed deal administrator personally squandered \$35 million. Ongoing cases of EB-5 investor fraud include a \$68 million Ponzi scheme involving a California oil company, a \$160 million convention center in Chicago and an alleged \$125 million fraud in two Seattle real estate projects. On April 28, it was revealed that Chinese investors have been fleeced of \$150 million in an Idaho gold mine fraud, and on April 6, a different fraud of \$50 million was alleged in California.

During his presidential campaign, Donald Trump repeatedly attacked China and warned about the dangers of deficient immigrant screening. If the Trump administration is serious about stopping illegal immigration, instead of building a costly thousand-mile wall, the EB-5 visa can and should be abolished now. ■

Bob Bauman is a former U.S. Congressman from Maryland. He is an author and lecturer on wealth protection, offshore residence and second citizenship. Email Bob at baumanletter@banyanhill.com

The Perils of Ignoring Debt

As you may know from past articles, I trained as an economist at university. Not *just* economics, though ... and like Robert Frost's road "less traveled by," that has made all the difference. I'm not so devoted to orthodoxy that I reject alternative viewpoints just because they don't "fit" what my professors told me.

One issue where I diverge from mainstream economists is on the role of debt in the macroeconomy.

The traditional view is that every loan is someone else's savings recycled. For that reason, debt is "neutral" with respect to the "real" economy of goods and services, with its business cycles and booms and busts. The latter must therefore be due to something other than finance.

In the orthodox view — I'm simplifying — recessions are caused either by endogenous shocks (like the oil crises of the '70s) or by leads and lags in the real economy.

Overproduction in a boom period leads to increased inventories, which triggers layoffs and reduces output, which causes a recession when lots of firms do it at once.

In the orthodox view, one thing that *doesn't* cause recessions is credit growth. Credit can lead to asset bubbles, and bubbles can pop, for sure. But analysis of the business cycle remains rooted in the supply and demand of goods and services. Debt is just a lubricant.

There are two problems with this.

First, given advances in information technology, just-in-time production and the destruction of unions, today's businesses have little reason to overshoot inventories.

They know perfectly well how much they need to have on hand and can adjust production on the fly. There simply isn't that much "stickiness" left in

the real economy to cause recessions on its own.

Second, it's painfully obvious that debt does have an impact on the real-world economy in three ways:

- **Cheap credit masks stagnating or declining real incomes.** During the 2000s, for example, U.S. consumers whose real incomes weren't rising were able to embark on an orgy of consumption that made them feel "prosperous." It also kept the economy growing. But when the financial system crashed in 2008, that accumulated debt had to be repaid ... at the expense of consumption, leading to a severe and ongoing recession in all sectors except investor assets.
- **Cheap money leads to an upward spiral of overinvestment in speculative assets like the stock market, real estate and intellectual property.** That in turn reduces the amount of money available for industrial investment, aggravating the real-economy recession ... and thus making industrial investment even less attractive. That's why we see so little new gross capital formation in the U.S. economy these days.
- **A high debt/GDP ratio means more national income is flowing to the owners of debt, undermining consumer demand.** When most debt is owned by a small elite of financial institutions and their shareholders, they accumulate a disproportionate share of national income and wealth, leaving less for everyone else for consumption and household investment (e.g., education) ... exactly what we see in today's U.S. economy.

Orthodox economists say that none of this matters. By definition, debt is owed to someone, who will eventually use debt repayments and interest earnings for consumption. But the tiny group that accumulates huge income from debt can't possibly consume enough to keep the whole economy healthy. Instead,

they reinvest it in more loans — or outside the U.S. economy altogether — which aggravates the problem.

Orthodox economics' biggest error is that lending is just recycled savings. If that were true, then the national accounts add up, and should achieve equilibrium most of the time.

In the orthodox view, the amount of money in the economy should always equal the value of real goods and services being produced and traded.

If that's true, excess "savings" can't be created out of thin air; they can only come from profitable productive activity. That means loans can't come from thin air, either.

But if banks can create money out of thin air — by issuing leveraged loans that investors use to chase assets like stocks or real estate — then there is no reason why the national economy should balance. Banks are creating new money by issuing loans that aren't backed by any deposits.

Quite the opposite: Such "bank originated money and debt" leads to overinvestment in nonproduced assets like stocks and real estate, as investors use leverage to increase their earnings through speculation.

Eventually, however, anything that causes asset prices to fall across the board — cash flow problems at an overleveraged investment bank, for example, or a political crisis — can lead to margin calls many investors can't meet.

This inevitably leads to a *systemic* crisis, as interlocked, overleveraged financial institutions shut down because money isn't flowing, either in the form of repayments or rollovers of short-term debt ... especially when that short-term money is used to back long-term borrowings, as is so often the case.

Nobody knows when this might happen — nobody saw it coming in 2008 — but it's critical to monitor the growth of debt in the economy as part of your wealth management strategy.

To my mind, the most important forms of debt to watch are margin debt and corporate debt.

Margin debt reflects the way investors are

leveraging their chase for yield by using borrowed money to buy stocks. It's especially dangerous for two reasons.

First, in a crisis, when stock values drop quickly, brokerages call in margin loans, forcing investors to liquidate other assets (such as gold) to cover these, forcing down prices of these assets as well.

Second, margin calls on heavily leveraged investors sometimes force them to borrow to cover them. But in a crisis, the short-term loaning market freezes, leading to defaults on margin calls — compounding the crisis in a negative spiral of unpaid debt.

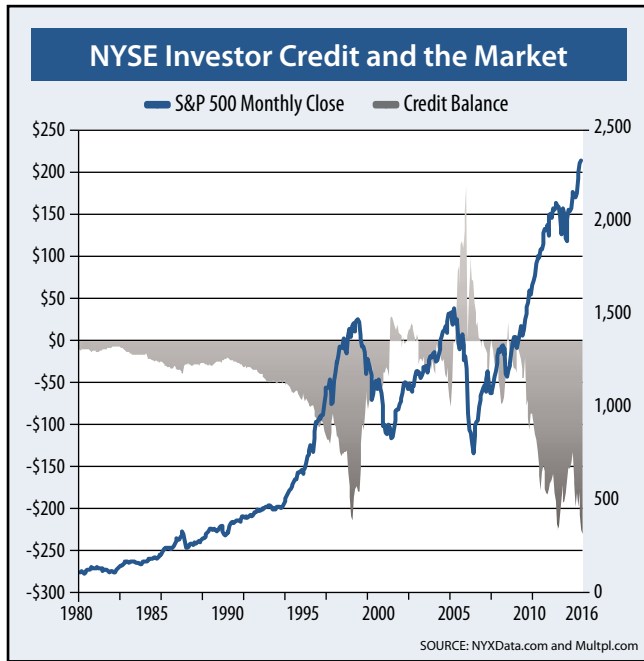
The following charts show the relationship between margin debt and the S&P 500 and the NYSE.

In the first, the rate of increase in margin debt exceeds the rate of increase in the S&P 500 itself — and the divergence between the two is growing rapidly, just as it did before the 2008 crash.



The second chart shows the same pattern for the NYSE.

The pattern is unmistakable. When margin debt starts to rise rapidly, a crash is coming. But it won't be caused by problems in the real economy of factories, restaurants and housing construction. Those could be doing just fine.



Instead, it will be a self-reinforcing cascade, as margin calls drain capital from investors, which leads to lower asset prices since nobody has enough liquidity to bid them up.

In fact, they'll need to sell to raise cash, making the problem worse. Declining stock indexes will wipe wealth off everybody's balance sheets, so they'll cut back on everything from buying cars to making corporate loans.

The second way debt threatens the economy is through corporate borrowing. A recent IMF report estimates that low interest rates have led U.S. firms to add \$7.8 trillion in debt and other liabilities since 2010.

These borrowings are not necessarily used to invest in new, job-creating lines of business, however, but to engage in financial engineering like stock buybacks, which goose the value of senior executives' stock options.

This heavy borrowing has led to leveraging levels in the energy, real estate, utilities, consumer discretionary, consumer staples and telecoms sectors that exceed the levels just preceding the 2008 financial crisis. Overall, U.S. corporate debt leveraging is 25% higher than in 2004-2006.

The IMF says:

The number of [U.S.] firms with very low interest coverage ratios – a common signal of distress – is already high: currently, firms accounting for 10% of corporate assets appear unable to meet interest expenses out of current earnings. This figure doubles to 20% of corporate assets when considering firms that have slightly higher earnings cover for interest payments, and rises to 22% under the assumed interest rate rise.

The stark rise in the number of challenged firms has been mostly concentrated in the energy sector, partly as a result of oil price volatility over the past few years. But the proportion of challenged firms has broadened across such other industries as real estate and utilities. Together, these three industries currently account for about half of firms struggling to meet debt service obligations and higher borrowing costs.

Overall,

Corporate credit fundamentals have started to weaken, creating conditions that have historically preceded a credit cycle downturn. Asset quality – measured, for example, by the share of deals with weaker covenants – has deteriorated. At the same time, a rising share of rating downgrades suggests rising credit risks in a number of industries.

The report notes that equity markets “have taken a relatively benign view” of the downside risks of U.S. corporate debt, and warns that there could be a “swift repricing of risks in the event of policy disappointment.”

If such a swift repricing of risks does occur, it will happen because debt *does* matter ... except, it seems, to the orthodox thinkers who oversee the U.S. financial system, who still think debt doesn't matter. ■

I'm interested in hearing more from you. What is your No.1 concern when it comes to your assets and your freedom? Send your comments to me at baumanletter@banyanhill.com

Does Puerto Rico's “Bankruptcy” Matter?

I N the April edition of *The Bauman Letter*, I advised you to consider taking advantage of Puerto Rico's unique tax advantages for mainlanders who relocate themselves — or their investment capital — to the island.

Some folks questioned my thinking, which is perfectly reasonable. I continue to believe that the Puerto Rican tax breaks aren't going to disappear, and that they could work well for some people. But it's an opinion, not a promise.

Then, last week, the government of Puerto Rico activated a clause in the Promesa Act that allows it to seek bankruptcy-like court protection from its creditors. Does this throw my whole logic out the window? Hardly. In fact, it was already “priced in” to my thinking.

The Puerto Rican government and its utility companies borrowed a lot of money on Wall Street after 2006. That's when the territory lost a previous advantageous tax status because congresspersons were unhappy at mainland corporations leaving their states and relocating to the island. This caused Puerto Rican tax revenues to tank.

But, Wall Street had an “artificial” incentive to lend the island's government money. The extra income they'd get from tax savings on Puerto Rican bonds offset the risk premium they'd normally apply. It was like free money — Wall Street catnip.

Still, Puerto Rico's economy continued to founder ... and then the 2008 crisis hit.

Paradoxically, the loans kept flowing because they were so (artificially) attractive to everyone involved. Even with heightened risk, Puerto Rican bonds remained attractive because, unlike U.S. municipal bonds (with which they are classed for tax purposes), the issuing government — Puerto Rico — isn't allowed to declare bankruptcy.

In other words, laws and regulations shaped market behavior and created perverse incentives — as they inevitably do.

Of course, the Puerto Rican government kept borrowing, so they are as much to blame as Wall Street. But decades of political maneuvering between Washington and San Juan had entrenched a dynamic of risk-taking, in the expectation that Congress would always step to fix the situation.

The problem is that the word is changing fast. Moving from Puerto Rico to the mainland used to mean being out of touch with family and friends back home. But with cheap fares, email, Skype and other ways to stay in virtual touch, moving stateside made more sense for many young Puerto Ricans.

The result is that the island lost nearly 10% of its population between 2000 and 2015. Most of these were working-age Puerto Ricans with skills and/or capital.

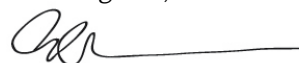
That's why I think Acts 20 and 22 will survive even under bankruptcy — because having people coming to the island and paying a low tax rate will generate revenue that otherwise wouldn't have existed. And given that most of the new arrivals are high-income, their total tax payments will be much larger than those of most Puerto Rican emigrants.

But Puerto Rico has another ace in the hole. It's not a state; it's a U.S. colony. If Puerto Ricans decide to withdraw their cooperation with Congress, they can do it. It wouldn't be easy ... but neither would sending in the U.S. armed forces to occupy and administer the territory. That wouldn't look good.

The alternative would be to grant Puerto Rico statehood, but that would probably mean two more Democrat senators in Washington, and as long as the GOP controls Capitol Hill, it's not likely to happen.

Puerto Rico's “bankruptcy” was expected. It doesn't change my opinion. In fact, it's a sign that the parties have accepted reality ... which, as everyone in a crisis knows, is the first step to recovery.

Kind regards,



Ted Bauman, Editor