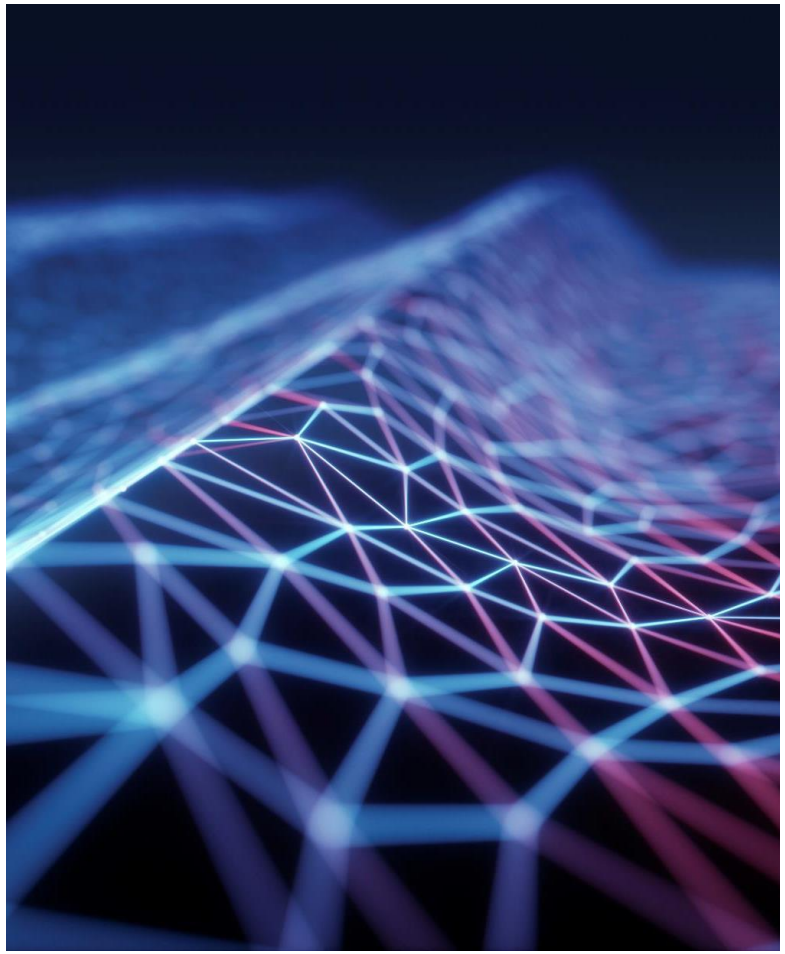
CYBER RISK IN THE TIME OF COVID

CYBER INSURANCE

WHAT YOU NEED TO KNOW NOW!



JOE SCULLY, PRESIDENT

FINANCIAL GUARANTY INSURANCE

COMPANIES BATTLE ANOTHER PANDEMIC*

SKYROCKETING HACKING ATTEMPTS

AS OF MAY 28TH THE FBI RECEIVED 230,000 COMPLAINTS, DOUBLE COMPARED TO THIS TIME LAST YEAR

WEAK PASSWORDS - SHARED LAPTOPS -INSUFFICIENT TRAINING ARE LIKELY THE ROOT OF THE ISSUE

* WALL STREET JOURNAL AUGUST 22, 2020

IBM CONDUCTED AN ONLINE SURVEY OF 2000 ADULTS NEWLY WORKING FROM HOME - JUNE 4-7 2020

43% HAD PERSONALLY IDENTIFIABLE INFORMATION.

45% SAID THEIR EMPLOYER HAD NOT PROVIDED SECURITY TRAINING FOR WORKING AT HOME.

37% REUSE PASSWORDS FOR BUSINESS AND PERSONAL APPLICATIONS.

53% SAY EMPLOYER HAS NO NEW SECURITY POLICY FOR MANAGING PERSONAL INFO WHEN WORKING AT HOME.

29% SAID THAT THEY LET THEIR KIDS AND OTHER FAMILY MEMBERS USE THEIR WORK LAPTOP FOR SHOPPING AND GAMING.

MOST BANKS HAVE THREE POLICIES THAT COVER CYBER EXPOSERS

- Financial Institution Bond – Computer Crime Insurance Agreement – Covering Money Stolen From the Bank by Hackers, Hacking into the Bank's Systems Directly or via Third Party Service Providers.

- Bankers Professional Liability – Depositors Liability – Most claims are primarily as a result of errors to safeguard customers money while on deposit.

- Cyber Insurance – Provides coverage for several cyber and privacy related issues.

CLAIMS STATISTICS*

6% OF ALL CLAIMS REPORTED ARE CYBER RELATED - SO FAR SO GOOD

24% ARE WIRE FRAUD OR OTHER ELECTRONIC CRIME (FI BOND) – STEALING FROM THE BANK

18% ARE WIRE FRAUD LIABILITY (DEPOSITOR LIABILITY) – ERRORS BY EMPLOYEES

18% ARE MEDIA AND WEBSITE (CYBER POLICY) – ADVERTISING, DENIAL OF SERVICE OR ADA ISSUES

17% ARE HACKER RELATED (CYBER POLICY) – MALWARE OR RANSOMWARE

16% ARE PRIVACY AND SECURITY (CYBER POLICY) – LOSS OR THEFT OF PERSONAL INFORMATION

7% OTHER CYBER CRIME (FI BOND) – PLASTIC CARD MOSTLY

* PROVIDED BY ABA INSURANCE SERVICES THAT CURRENTLY INSURES APPROXIMATELY 1500 COMMUNITY BANKS AS OF JUNE 2020

CYBER FIRST PARTY COVERAGE – INSUREDS OUT OF POCKET

- Privacy and Security Breach Expenses – Indemnifies the insured for expenses incurred to remediate breaches, ransomware or denial of services Attacks.

- Pays For Forensic Investigations – Restoration costs - Legal Counsel – Notification Costs – Plastic Card Reissuance – Credit and Identity Monitoring.

- Most carriers provide access to consultants and legal counsel to guide the insured thru the process.

This is important, with the expenses covered and advice from consultants the insured can respond quickly and confidently. Potentially reducing the possibility of big liability losses and minimizing the bank reputation risk.

CYBER LIABILITY COVERAGE

- Cyber Liability covers legal costs when the insured receives a demand or is named in a lawsuit requesting compensation for damages.
- Some carriers will provide legal representation and some carriers will allow the insured to choose.
- Cyber events are defined as breaches into the banks system, loss of confidential with no breach like a loss of a laptop, confidential papers, hacks into vendors systems, employee confidential (HIPPA) info
- Denial of Service Attacks – customers can not access the banks system
- Website advertising or non hosted sites like Facebook or LinkedIn

CLAIMS ACTIVITY

HELOC FRAUD

WIRE FRAUDS – SOCIAL ENGINEERING

ATM FRAUD

THEFT OF PERSONAL INFORMATION

EMAIL SPEARFISHING

THINGS TO CONSIDER

1. REGULAR TRAINING OF YOUR EMPLOYEES ON SECURITY PROTOCOLS IS VITAL.

2. MAKE SURE THAT EMPLOYEES ARE LIMITING ACCESS BY OTHERS TO THEIR WORK COMPUTERS.

3. MAKE SURE EMPLOYEE DEVICES HAVE UPDATED CYBER PROTECTION SOFTWARE.

4. MAKE SURE EMPLOYEES WORKING AT HOME USE WORK-PROVIDED VPN'S.

THINGS TO CONSIDER

5. Shred any documents printed at home that are not necessary.

6 Report any lost or stolen devices ASAP.

7. Make sure your employees know the protocol if an off-site issue comes up.

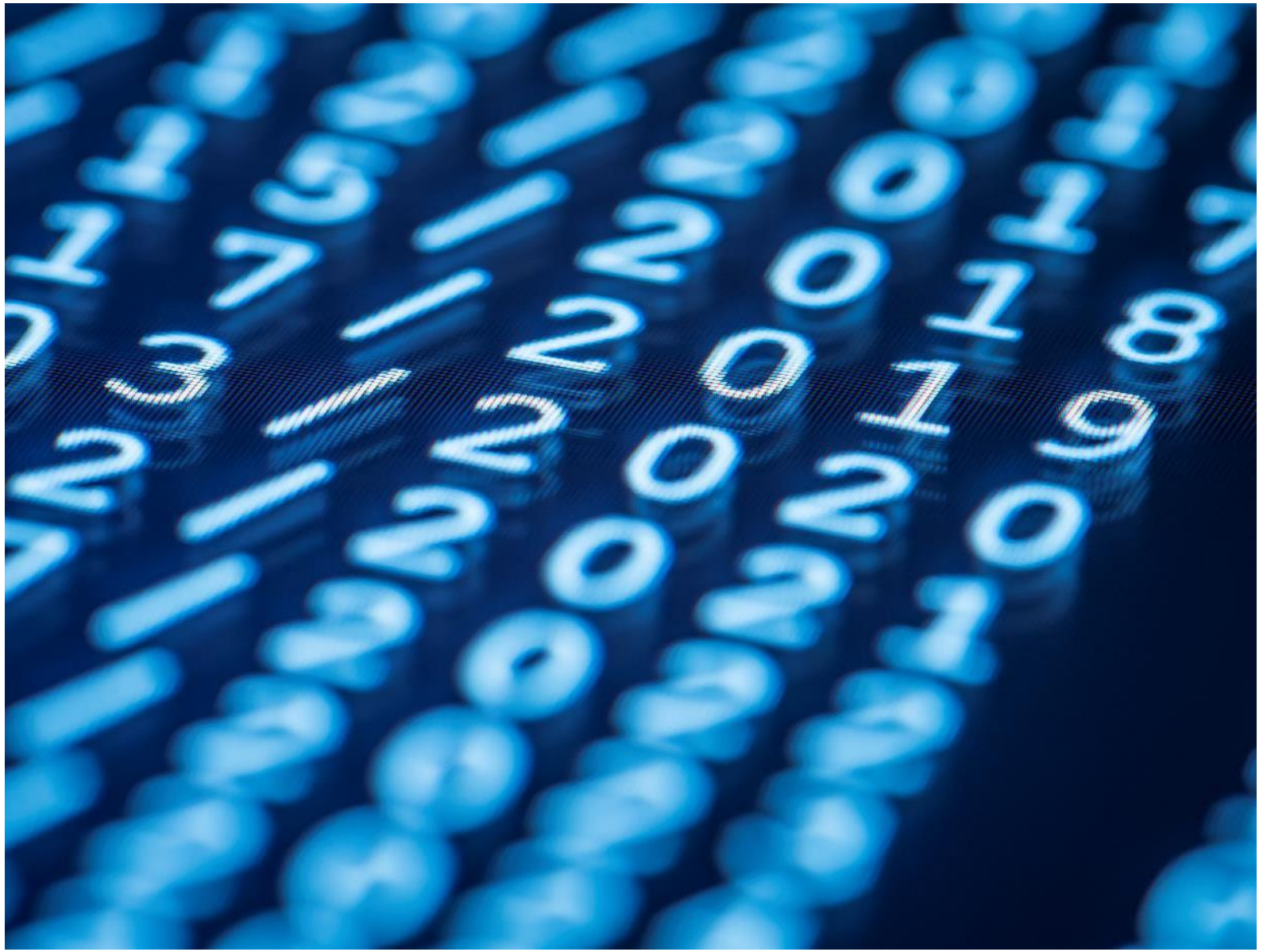
IN CONCLUSION

It is clear regulated Financial Institutions do a good job of protecting their confidential information based on loss data. Continue to be diligent.

It's a matter of when, not if your bank will have Cyber Related issue have a strong response plan. Know what to do when it happens. Don't be a deer in the headlights.

Consider where your capital is being directed if you are feeling confident your banks Cyber Security Program is strong maybe look at other areas where the bank maybe vulnerable.

QUESTIONS?



THANK YOU

JOE SCULLY

626-893-7800

JOES@FGIB.COM