WEIS 2004

An Insurance Style Model for Determining the Appropriate Investment Level against Maximum Loss arising from an Information Security Breach

Roger Adkins
School of Accountancy, Economics & Management Science
University of Salford
Greater Manchester M5 4WT UK

r.adkins@salford.ac.uk
Traditional Capital Budgeting

\[
NPV = \sum_{t \text{ all possible values of } t}^{\text{planning horizon}} \frac{\lambda E[L]}{(1+k)^t} - I
\]

I  Investment in information security

E[L]  Change in expected loss from introducing investment at level I

\lambda  Probability of a breach

k  Appropriate discount rate

t  Time
Traditional Capital Budgeting

$$\text{NPV} = \sum \frac{\lambda E[L]}{(1+k)^t} - I$$

Select the level of I to optimise NPV

Level of I has to influence one or both of:

- Distribution of L
- Value of $\lambda$

Appropriate value of $k$

- Reflect riskiness of future cash flows
Investment model:

- Inclusion of time
- Distribution of losses
- Possibility of multiple breaches within planning horizon
- Appropriate discount rate

Level of investment influences the distribution of losses

- Later, allow investment level to influence $\lambda$
Investment in information security limits the maximum loss from a security breach to $Q$

Savings from the investment $= \max\{ L - Q, 0 \}$

Conceptualise model as binomial option pricing framework
- Apply standard binomial option pricing theory
- Extend binomial model to continuous equivalent
Model Notation

L  Loss incurred when breach occurs
L^+  Upper loss with probability p
L^-  Lower loss with probability 1- p
\lambda  Probability of a breach per unit period
F  Investment in information security

Consider a small interval \Delta t
Define:
\tau = n\Delta t
T = N\Delta t where N > n
Conceptual Model

\[
(1 - \lambda \Delta t) \rightarrow \lambda \Delta t \rightarrow \lambda \Delta t \rightarrow p \rightarrow 1 - p \rightarrow \Delta t \rightarrow L_t^+ \rightarrow L_t^- \rightarrow \Delta t \rightarrow T = N \Delta t
\]
Assume $\lambda$ and $p$ are independent.
Set $\Delta t=1$ with no loss in model complexity
Value of investment $F$ to confer a degree of protection against breach such that firm suffers no greater loss than $Q$

$F^+_1 = \max\{L^+_1 - Q, 0\}$

$F^-_1 = \max\{L^-_1 - Q, 0\}$

Not possible to discount expected value at risky rate
Twin security (spanning portfolio) $S$ exists perfectly correlated with $L$. 

Diagram:

- $S_0$ at $t = 0$
- $S_1^+$ at $t = 1$
- $S_1^-$ at $t = 1$

Transition probabilities:
- $p$ from $S_0$ to $S_1^+$
- $1-p$ from $S_0$ to $S_1^-$
Construct a portfolio composed of buying \( m \) units of \( S \) partially funded through borrowing \( B \) at riskless rate \( r \)

\[
F_0 = mS_0 - B
\]

\[
F_1^+ = mS_1^+ - (1 + r)B
\]

\[
F_1^- = mS_1^- - (1 + r)B
\]

Solve for \( m \) and \( B \)
Conceptual Model

\[
m = \frac{F_1^+ - F_1^-}{S_1^+ - S_1^-}
\]

\[
B = \frac{mS_1^- - F_1^-}{1 + r}
\]

\[
F_0 = mS_0 - B
\]

\[
q = \frac{(1 + r)S_0 - S_1^-}{S_1^+ - S_1^-}
\]

\[
F_0 = \frac{qF_1^+ + (1 - q)F_1^-}{1 + r}
\]
Create a binomial lattice with \( n (=9) \) steps

At each final node, derive \( F^s_n \) and apply certainty equivalent probabilities and riskless rate to determine present value of \( F \)

Allow \( n \) to become very large
Derive $F_0$ from the Binomial probability model
Equivalently apply the log-normal approximation

$$F_0 = L_0 N(x) - Q(1+r)^{-\tau} N(x - \sigma \sqrt{\tau})$$

$$x = \frac{\ln \left( \frac{L_0}{Q(1+r)^{-\tau}} \right)}{\sigma \sqrt{\tau}} + 0.5 \sigma \sqrt{\tau}$$

Define $u = S_1^+ / S_0$ and $d = S_1^- / S_0$ where $d = 1/u$

$$\sigma = \ln(u) / \sqrt{h}$$

$h$ is length of period from 0 to 1, $h = \tau / n$
Conceptual Model

\[ F_0 = L_0 N(x) - Q(1+r)^{-\tau} N(x - \sigma \sqrt{\tau}) \]

Black – Scholes option pricing formula

- \( F_0 \) is value of European call option
- Exercise (strike) price \( Q \)
- Time to expiration is \( \tau \)

\( F_0 \) denotes the cost of protection against a loss of at least \( Q \)

Loss only occurs at time \( \tau \)

Assumes a breach will take place
\[
(1 - \lambda \Delta t) + \lambda \Delta t p + (1 - p) L^- + \Delta t L^+ = \Delta t (1 - \lambda \Delta t) + \lambda \Delta t p + (1 - p) L^- + \Delta t L^+ = T = N \Delta t
\]
Conceptual Model

\[ S_0 = 0 \]

\[ (1 - q') \]

\[ q' \]

\[ S_1^+ = 0 \]

\[ S_1^- \]

\[ t = 0 \]

\[ t = \Delta t \]

\[ S_0 = \frac{E[S_i^s]}{1 + r\Delta t} = \frac{(1 - q')S_1^+ + q'S_1^-}{1 + r\Delta t} \]

\[ = \frac{q'S_1^-}{1 + r\Delta t} \]

\[ \lambda \Delta t \approx S_0 / S_1^- \]

\[ q' = \lambda \Delta t(1 + r\Delta t) \approx \lambda \Delta t \]
Conceptual Model

Probability of a breach at \( t = n\Delta t \)

Probability of a breach at stage \( n \), preceded by \( j \) breaches and \( (n-j-1) \) no breaches in a specified order:

\[
= (\lambda \Delta t)^j (1 - \lambda \Delta t)^{n-1-j} \lambda \Delta t
\]

Probability of a breach at stage \( n \), preceded by \( j \) breaches and \( (n-j-1) \) no breaches in any order:

\[
= \binom{n-1}{j} (\lambda \Delta t)^j (1 - \lambda \Delta t)^{n-1-j} \lambda \Delta t
\]

Probability of a breach at stage \( n \):

\[
= \sum_{j=0}^{n-1} \binom{n-1}{j} (\lambda \Delta t)^j (1 - \lambda \Delta t)^{n-1-j} \lambda \Delta t = \lambda \Delta t
\]
Conceptual Model

\( F_0(Q, t) \) denotes the cost of protection against a maximum loss of \( Q \)

Loss only occurs at time \( t = n\Delta t \)

Assumes a breach will take place.

Cost of protection against a maximum loss of \( Q \) at time \( t = n\Delta t \):

\[ = \lambda\Delta t \times F_0(Q, t) \]

Cost of protection against a maximum loss of \( Q \) over horizon \( t=0 \) to \( t=T \):

\[ = \int_0^T \lambda F_0(Q, t)dt \]
Profiles

Profile of $F_0$ against time (years)

$L_0 = 120$  \hspace{1cm} r = 5\% \hspace{1cm} \sigma = 2$

$Q = 80$ \hspace{1cm} $Q = 120$ \hspace{1cm} $Q = 160$
Profile of $F_0$ against time (years)

$L_0 = 120$  \quad  \quad  r = 5\%  \quad  \quad  Q = 120$

\[ \sigma = 1.5 \quad \sigma = 2.0 \quad \sigma = 2.5 \]
Profiles

Cost of protection against a maximum loss $Q$ over horizon $t=0$ to $t=T$: 

$$ = \int_{0}^{T} \lambda F_0(Q, t) dt $$

Define $H_0$ as integral of $F_0$ over interval $t=0$ to $t=T$: 

$$ H_0 = \int_{0}^{T} F_0(Q, t) dt $$
Profile of $H_0$ against time (years)

$L_0 = 120 \quad r = 5\% \quad \sigma = 2$

Lines:
- $Q = 80$
- $Q = 120$
- $Q = 160$
Profile of $H_0$ against time (years)

$L_0 = 120$  \hspace{1cm}  $r = 5\%$  \hspace{1cm}  $Q = 120$

$\sigma = 1.5$  \hspace{1cm}  $\sigma = 2.0$  \hspace{1cm}  $\sigma = 2.5$
Investment Level Influences $\lambda$

Cost of protection against a loss of at least $Q$ over horizon $t=0$ to $t=T$:

$$I_0 = \int_0^T \lambda f_0(Q, t) \, dt = \lambda H_0$$

Assume:

$$\lambda = \lambda_0^{(a I_0 + 1)}$$

Cost of protection against a loss of at least $Q$ over horizon $t=0$ to $t=T$:

$$I_0 = \lambda_0^{(a I_0 + 1)} \times H_0$$
Profile of $I_0$ against Lambda-zero

$H_0 = 100$

$\alpha = 0.05$

$\alpha = 0.10$

$\alpha = 0.25$
Conclusions

Maximum loss

• Lowering the maximum loss incurred increases the investment level

Planning horizon

• Investment level is non-linear in short term

NPV or time dependent framework

• Apply the justified appropriate discount rate

Expectation of loss is important

• BUT, so is the variability
Discussion

• Twinning security
• Independence between $\lambda$ and $p$
• Firm investment behaviour
• Investment allocation
• Benefit function
Twinning Security

What is at risk?

• Theft and fraudulent acquisition of assets
• Reputation
• Information integrity
• Operational breakdown and failures
• Compensation
• Resources to revive normality

Adopt real options framework
• Use subjective estimates

Extent that loss correlated with firm’s equity
Independence between $\lambda$ and $p$

Treatment of $\lambda$ as a constant

Independence condition can be relaxed

P Boyle (1988)
A Lattice framework for option pricing with two state variables
Journal of financial and Quantitative Analysis, 23 1-26

Mathematically more complicated
Firm Investment Behaviour

Assumption of firm rationality

Prospect Theory: D Kahneman and A Tversky (1979), D Kahneman, J Knetschen and R Thaler (1991)

Firms adopt risk-loving solution in the face of losses

- Preference for uncertain higher loss than a certain lower loss
- Risk aversion falls after a period of zero security breaches
- Risk aversion increases after a security breach
- Risk loving to recoup a substantial past loss
Investment Allocation

Apportionment of investment across information security devices and mechanisms

- Upfront versus continuous expenditures

- Division between mitigating losses and probability reduction
Benefit Function

Future benefits from investment akin to insurance

- Inappropriate

- Investigations with random benefits
An Insurance Style Model for Determining the Appropriate Investment Level against Maximum Loss arising from an Information Security Breach

Roger Adkins
School of Accountancy, Economics & Management Science
University of Salford
Greater Manchester M5 4WT UK

r.adkins@salford.ac.uk